DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ADONIS HERNANDEZ VELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
NEIVA HUILA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ADONIS HERNANDEZ VELA

Diplomado de opción de grado presentado para optar
el título de INGENIERO *ELECTRONICO/SISTEMAS/TELECO*

DIRECTOR:

MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
NEIVA HUILA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

NEIVA-HUILA, 26 de junio de 2022

AGRADECIMIENTOS

Agradecimientos a la universidad nacional por darnos la oportunidad de podernos certificar en cisco en el aprendizaje en CCNA y darnos la oportunidad de realizar de paso el proyecto como opción de grado a nosotros como estudiantes de la universidad, optando de que los estudiantes aprendan de tecnologías acorde a su carrera o programa de formación.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

DNS: La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

INTERFAZ: Se conoce como Interfaz Física a los medios utilizados para la conexión de un computador con el medio de transporte de la red.

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

PROTOCOLOS DE RED: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

PREFIJO IP: conocido como “protocolo de internet “Es una forma particular de expresar las direcciones de red y sus máscaras a partir de identificar solamente la cantidad de bits que se encuentran en uno en la máscara de subred.

ROUTER: Dispositivo hardware software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

SWITCH: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3)

RESUMEN

La evaluación en el cual se denominará “Prueba de habilidades prácticas”, forma parte de las actividades finales y evaluativas del Diplomado de Profundización CCNA como opción de grado, y busca identificar el nivel de desarrollo de competencias y habilidades en el cual fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y habilidades para la solución de problemas relacionados con diversos aspectos en el campo de Networking. En el primer escenario se configurarán los dispositivos tales como switches router y computadores formando una red pequeña denominado LAN. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 en el cual el enrutamiento se deriva con los últimos dígitos de la cedula Cada estudiante tomará el direccionamiento 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts). En el Segundo escenarios configura tres routes y dos switch donde también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Para el segundo 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 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, también se configurara un pool de direcciones. Y un acceso de lista también se configurará un lookback.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

The evaluation in which it is called "Practical skills test", is part of the final and evaluative activities of the CCNA Deepening Diploma as a degree option, and seeks to identify the level of development of skills and abilities in which they were acquired throughout length of the diploma. The essential is to test the levels of understanding and problem solving skills related to various aspects in the field of Networking. In the first scenario, devices such as router switches and computers will be configured to form a small network called lan. You must configure a router, a switch and equipment that supports both IPv4 connectivity in which the routing is derived with the last digits of the ID Each student will take the address 192.168.X.0 where X corresponds to the last two digits of their ID With the provided address, it will perform subnetting and fulfill the requirement for LAN1 (100 hosts) and LAN2 (50 hosts). In the second scenario, three routes and two switches are configured where they must also be managed securely. You will configure routing between VLANs, DHCP, Etherchannel, and port-security. For the second scenario, a small network must be configured to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), address translation of dynamic and static network (NAT), access control lists (ACL) and network time protocol (NTP) server/client, a pool of addresses is also configured. And a list access will also configure a lookback.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Este trabajo se desarrollará de acuerdo a tres escenarios en el cual se configurará de acuerdo a las siguientes especificaciones:

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PC. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

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 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. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología escenario 1.

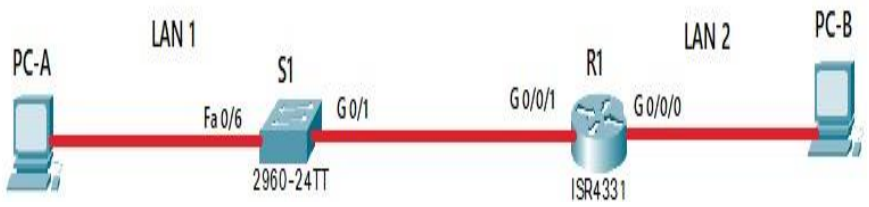
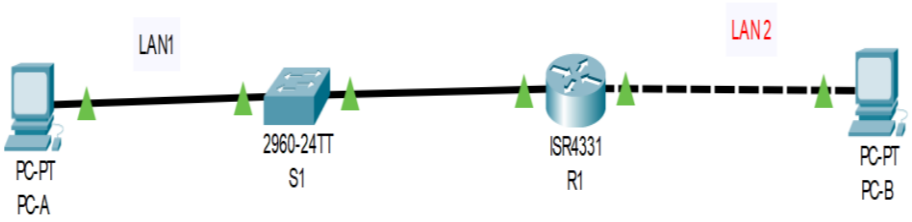


Figura 2. Simulaciones de escenario 1



Fuente: Propia

Objetivos del escenario

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red del escenario 1

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.**17**.0 donde

Tabla 1. Guía de direccionamiento.

Item	Requerimiento
Dirección de Red	192.168.17.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100 192.168.17.1/255.255.255.128
Requerimiento de host Subred LAN2	50 192.168.17.129/255.255.255.192
R1 G0/0/1	Primera dirección de host de la subred LAN1 ip address 192.168.17.1 255.255.255.128
R1 G0/0/0	Primera dirección de host de la subred LAN2 ip address 192.168.17.129 255.255.255.192
S1 SVI	Segunda dirección de host de la subred LAN1 ip address 192.168.17.2 255.255.255.128
PC-A	Última dirección de host de la subred LAN1 192.168.17.126 255.255.255.128
PC-B	Última dirección de host de la subred LAN2 192.168.17.190 255.255.255.192

Fuente: Prueba de habilidades CCNA 2022.

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración R1.

Tarea	**Especificación**
Desactivar la búsqueda DNS	#no ip domain-lookup
Nombre del router	#hostname R1
Nombre de dominio	#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	#enable password ciscoenpass
Contraseña de acceso a la consola	#line console 0 #password Cisconas #login local
Establecer la longitud mínima para las contraseñas	#security password min-length 10
Crear un usuario administrativo en la base de datos local	#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	#line vty 0 4 # password ciscoenpass # login local
Configurar VTY solo aceptando SSH	# transport input ssh
Cifrar las contraseñas de texto no cifrado	

Configure un MOTD Banner	#banner motd “SE PROHÍBE EL ACCESO NO AUTORIZADO.”
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	# crypto key generate rsa general-Keys modulus 1024

Fuente: Prueba de habilidades CCNA 2022

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Tabla Configuración S1.

Tarea	**Especificación**
Desactivar la búsqueda DNS.	#no ip domain-lookup
Nombre del switch	#hostname **S1**
Nombre de dominio	#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	#enable password ciscoenpass
Tarea	**Especificación**
Contraseña de acceso a la consola	#line console 0 #password Cisconas #login local
Crear un usuario administrativo en la base de datos local	#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	#line vty 0 4 # password ciscoenpass

	# login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	# transport input ssh
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	#banner motd “SE PROHÍBE EL ACCESO NO AUTORIZADO.”
Generar una clave de cifrado RSA	# crypto key generate rsa general-Keys modulus 1024
Configurar la interfaz de administración (SVI)	# interface VLAN 98 # ip address 192.168.17.2 255.255.255.128 # no shutdown
Configuración del gateway predeterminado	#ip default-gateway 192.168.17.1

Fuente: Prueba de habilidades CCNA 2022

Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4. Configuración PC-A.

PC-A Network Configuration	
Descripción	*en blanco*
Dirección física	*192.*192.168.17.0/25*26*
Dirección IP	192.168.17.126/25
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.17.1/25

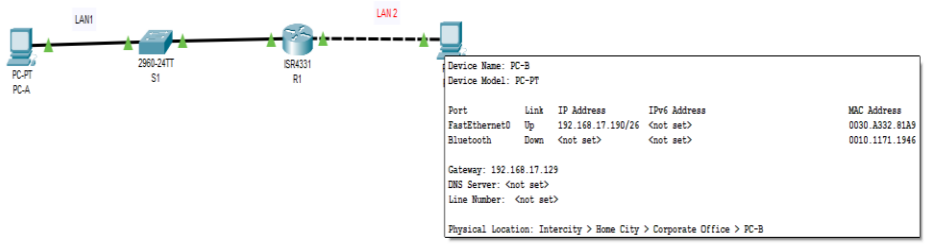
Fuente: Prueba de habilidades CCNA 2022

Tabla 5. Configuración PC-B.

PC-B Network Configuration	
Descripción	*en blanco*
Dirección física	192.168.17.0/26
Dirección IP	192.168.17.190/26
Máscara de subred	255.255.255.192
PC-B Network Configuration	
Gateway predeterminado	192.168.17.1/26

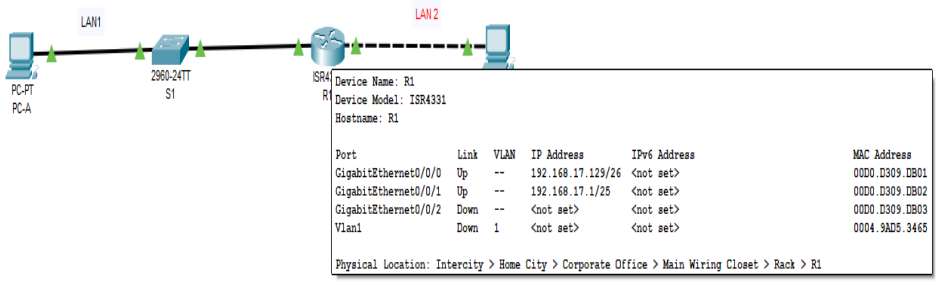
Fuente: Prueba de habilidades CCNA 2022

Figura 3. Tabla de enrutamiento PC-B escenario 1.



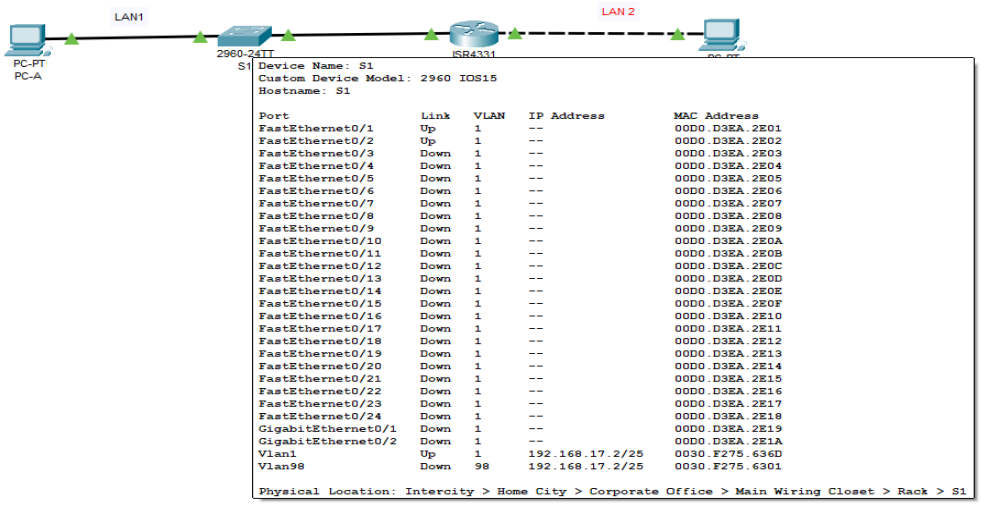
Fuente: Propia

Figura 4. Tabla de enrutamiento R1 escenario 1.



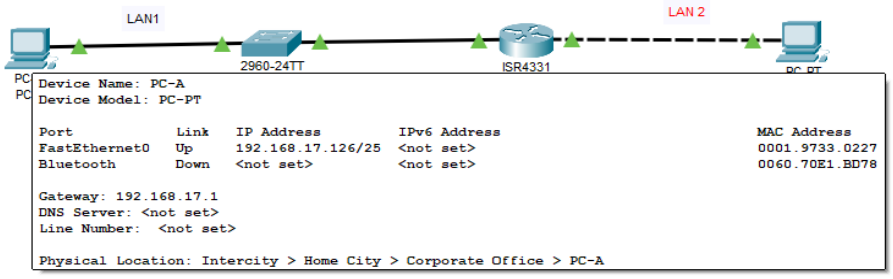
Fuente: Propia

Figura 5. Tabla de enrutamiento S1 escenario 1.



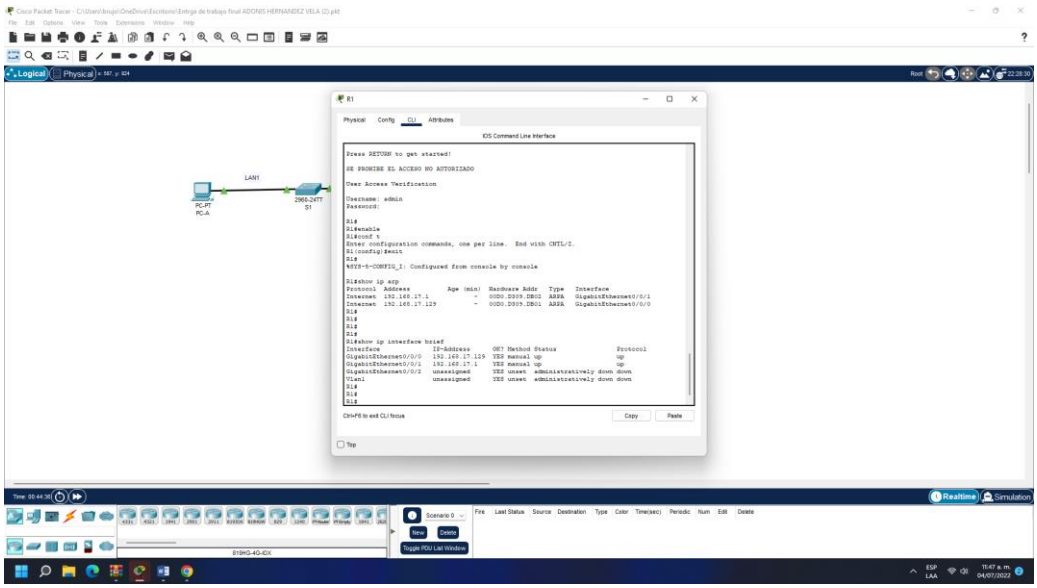
Fuente: Propia

Figura 6. Tabla de enrutamiento PC-B escenario 1.

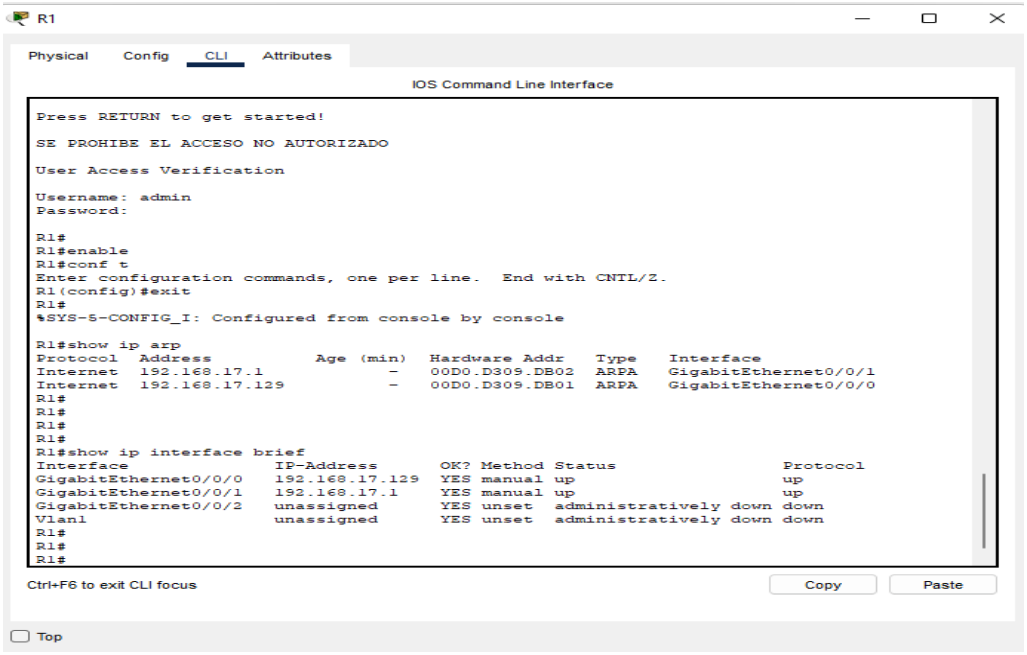


Fuente: Propia

Figura 7. Comandos show ip arp y show ip interface brief en R1 escenario 1

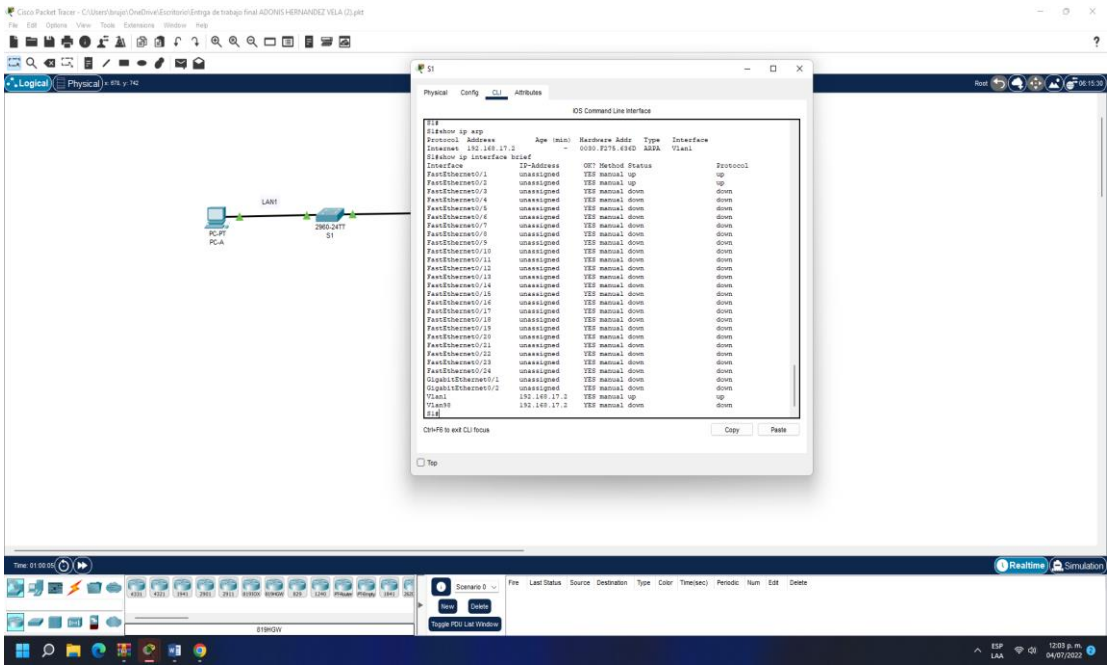


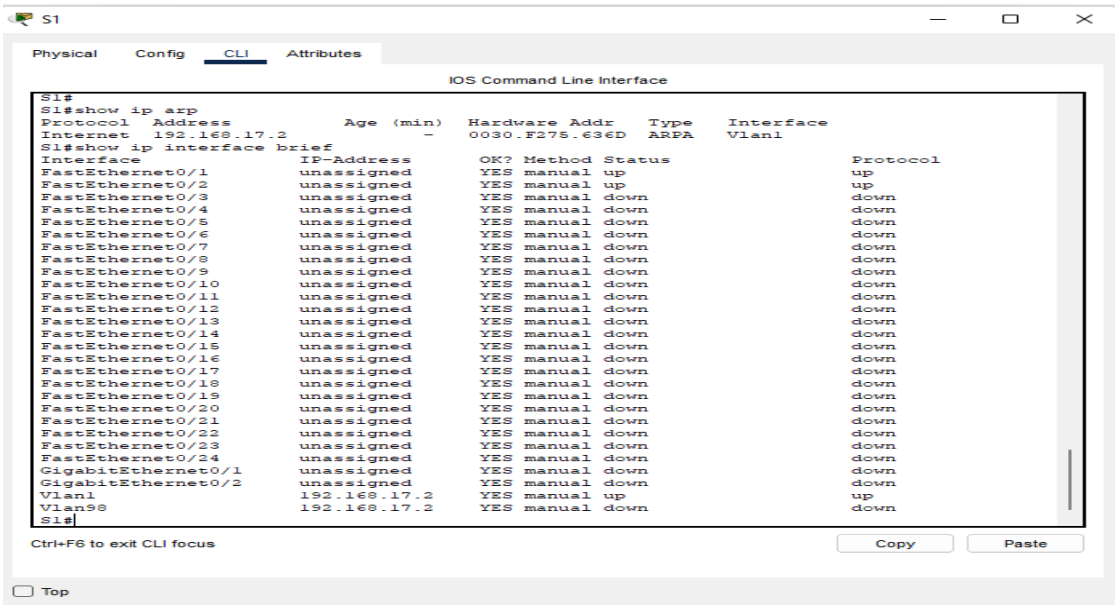
Fuente: Propia



Fuente: Propia

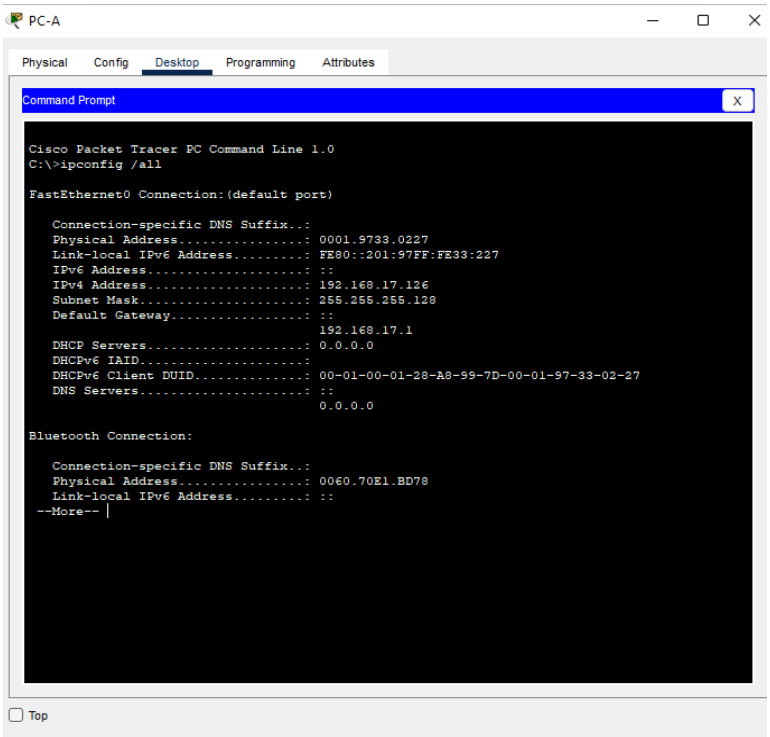
Figura 8. Comandos show ip arp y show ip interface brief en S1 escenario 1.





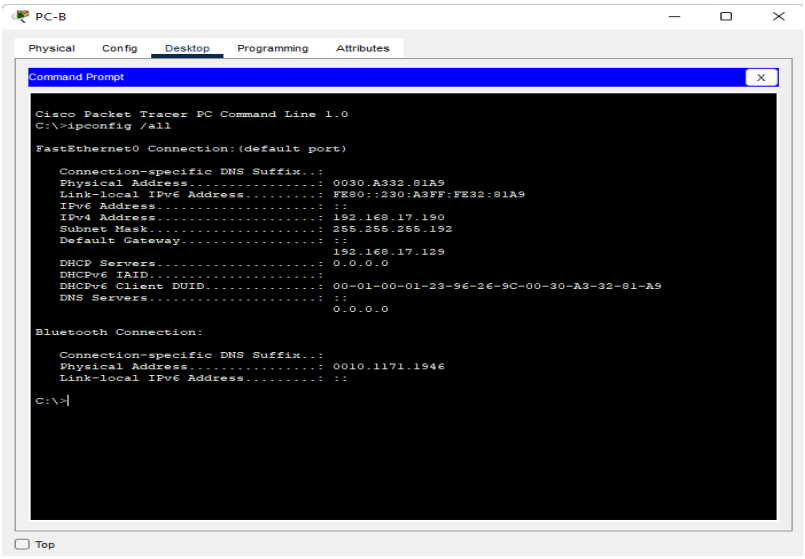
Fuente: Propia

Figura 9. Comando ipconfig /all en PC-A escenario 1



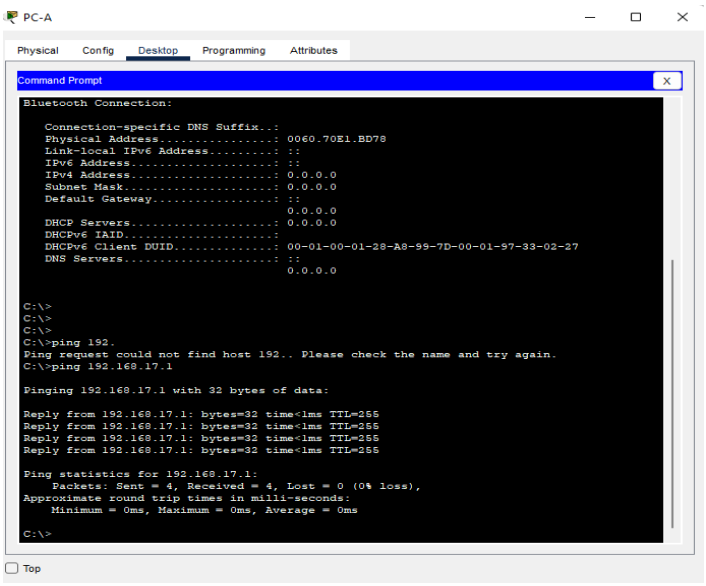
Fuente: Propia

Figura 10. Comando ipconfig /all en PC-B escenario 1



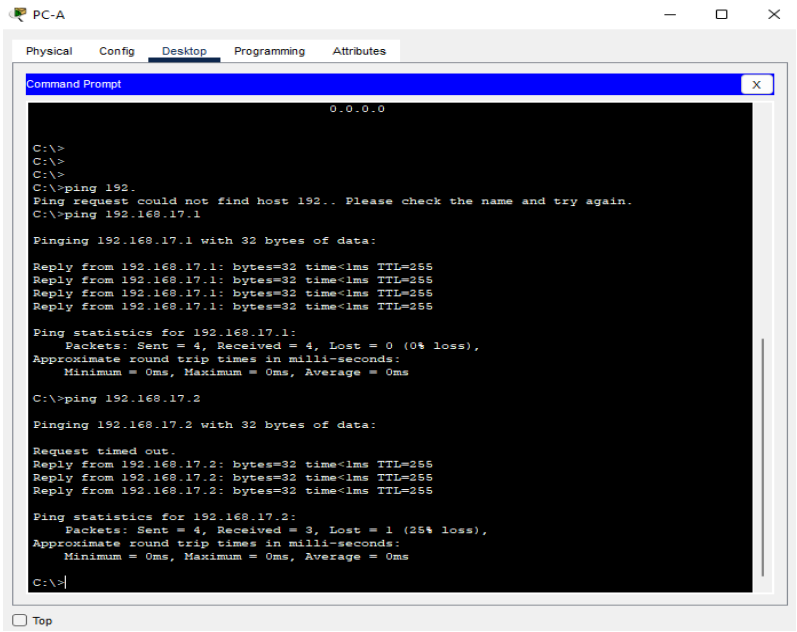
Fuente: Propia

Figura 11. Prueba de Conectividad PC-A a R1 escenario 1.



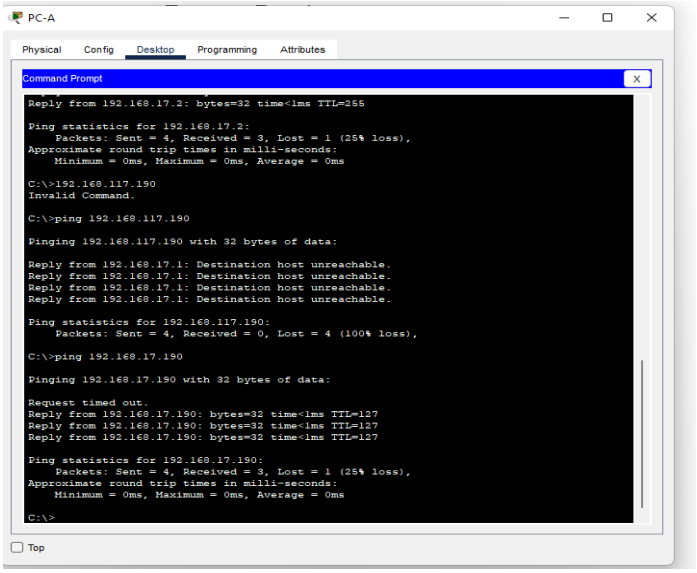
Fuente: Propia

Figura 12. Prueba de Conectividad PC-A a S1 escenario 1.

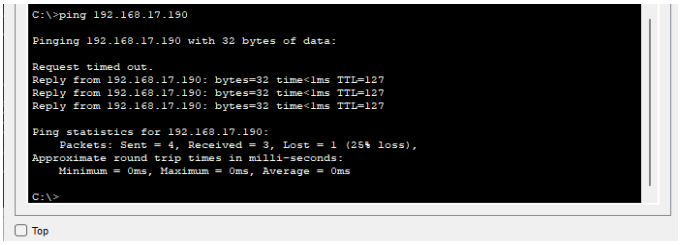


Fuente: Propia

Figura 13. Prueba de Conectividad PC-A a PC-B escenario 1.

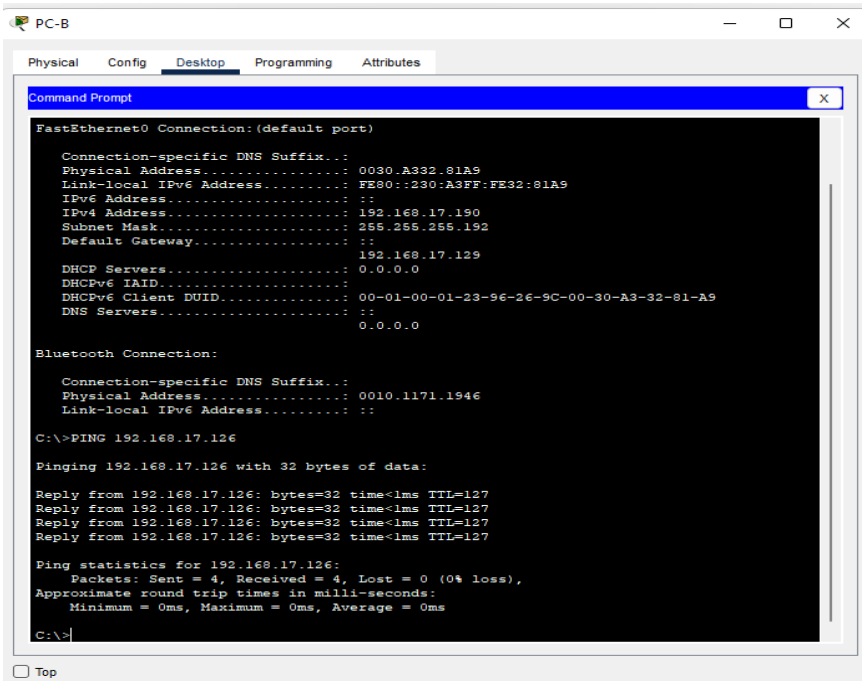


Fuente: Propia



Fuente: Propia

Figura 14. Prueba de Conectividad PC-B a PC-A escenario 1.



Fuente: Propia

DESARROLLO

2. Escenario 2

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 OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de

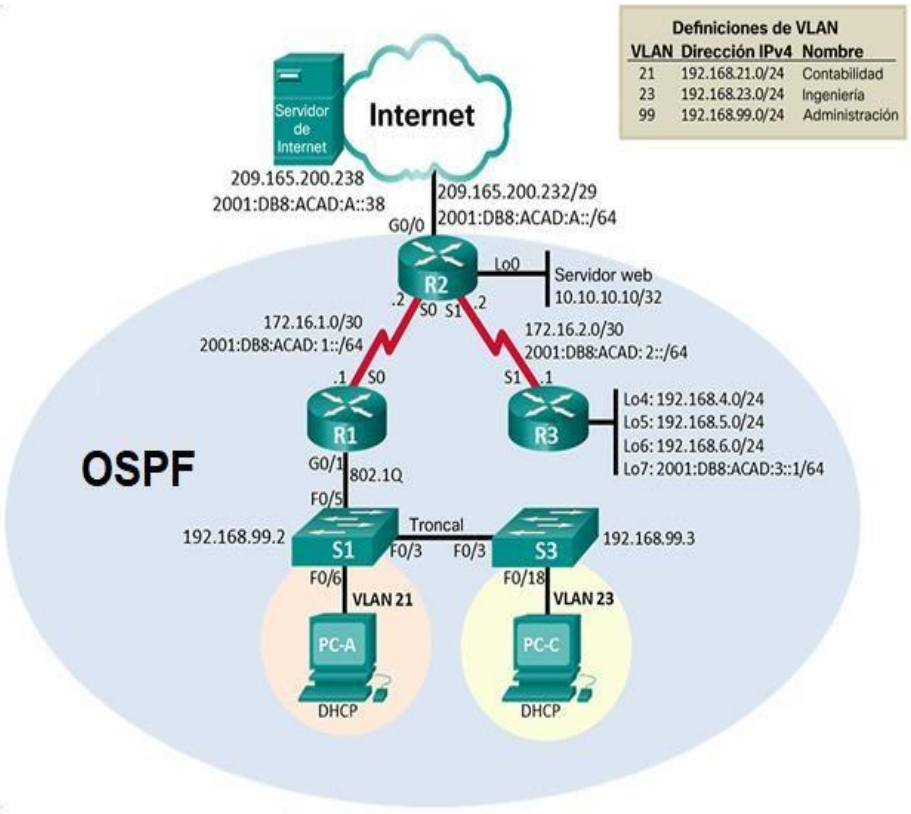
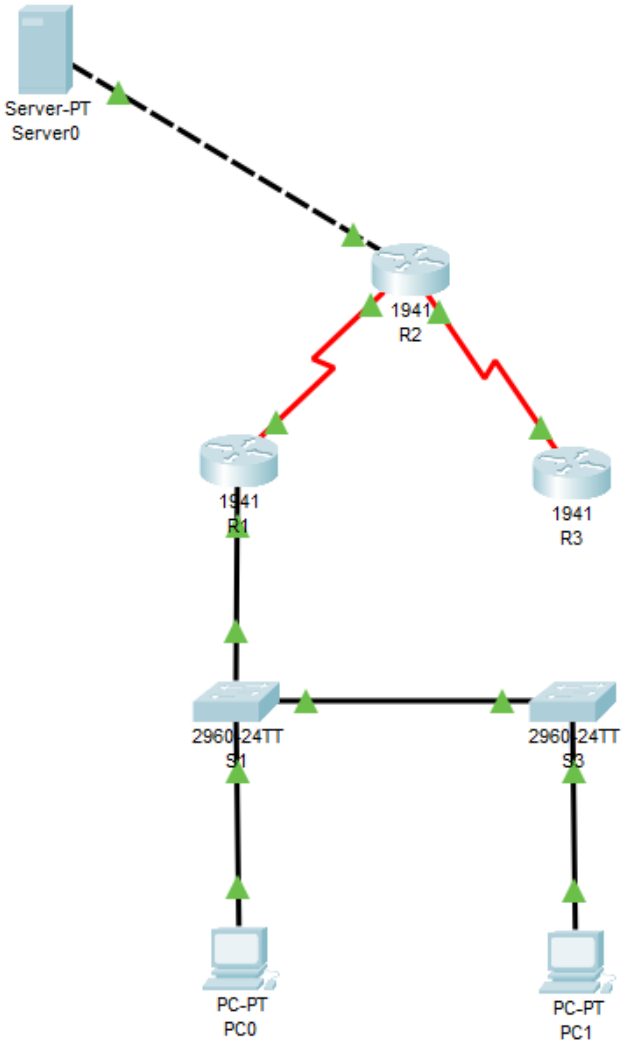


Figura 15. Topologia del escenario 2



Fuente: Propia

Parte 1: Inicializar dispositivos.

Paso 1: Inicializar y volver a cargar los routers y los switches. Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 6. Inicializar dispositivos.

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Erase startup-config Delete vlan.dat
Volver a cargar ambos switches	reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Show flash

Fuente: Prueba de habilidades CCNA 2022

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 7. Parámetros básicos de los dispositivos.

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Prueba de habilidades CCNA 2022

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

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

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1# configure terminal R1(config)# interface S0/0/0 R1(config)#description connection to R2 R1(config-if)# ip add 172.16.1.1 255.255.255.252 R1(config-if)# ipv6 add 2001:DB8:ACAD:A::a/64 R1(config-if)# clock rate 128000 R1(config-if)# no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1 (config)# ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1 (config)# ipv6 route ::/0 s0/0/0

Fuente: Prueba de habilidades CCNA 2022

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	# no ip domain-lookup
Nombre del router	R2 hostname R2
Contraseña de exec privilegiado cifrada	class # enable secret class
Contraseña de acceso a la consola	cisco R2#configure terminal R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit
Contraseña de acceso Telnet	Cisco R2#configure terminal R2(config)#line vty 0 4 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R2(config-line)# service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado. # banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.

	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2#interface S0/0/0 R2(config-if)# description connection to R1 R2(config-if)# ip address 172.16.2.1 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:1::2/64 R2(config-if)# no shutdown R2(config-if)# exit
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2# configure terminal R2(config)# interface S0/0/1 R2(config-if)# description connection to R3 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:2::2/64 R2(config-if)# clock rate 128000 R2(config-if)# no shutdown R2(config-if)# exit
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2# configure terminal R2(config)# interface G0/0

	R2(config-if)#description connection to internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)# ipv6 address 2001:db8:acad:a::1/64 R2(config-if)# no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)# interface loopback 0 R2(config-if)# ip address 10.10.10.10 255.255.255.0 R2(config-if)#description servidor web simulado R2(config-if)# exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Fuente: Prueba de habilidades CCNA 2022

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Hostname R3
Contraseña de exec privilegiado cifrada	class R3(config)# enable secret class
Contraseña de acceso a la consola	cisco R3#configure terminal R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit
Contraseña de acceso Telnet	cisco R3#configure terminal R3(config)#line vty 0 4 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config) banner motd “Se prohíbe el acceso no autorizado”

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3# configure terminal R3(config)# interface S0/0/1 R3(config-if)# description connetion to R2 R3(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# ipv6 address 2001:db8:acad:1::2/64 R3(config-if)# no shutdown R3(config-if)# exit
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	

Fuente: Prueba de habilidades CCNA 2022

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	Hostname S1
Contraseña de exec privilegiado cifrada	class S1(config)# enable secret class
Contraseña de acceso a la consola	cisco S1#configure terminal S1(config)#line console 0 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit
Contraseña de acceso Telnet	cisco S1#configure terminal S1(config)#line vty 0 4 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S1(config) banner motd “Se prohibe el acceso no autorizado”

Fuente: Prueba de habilidades CCNA 2022

Paso 6: Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración S3.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)# no ip domain-lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	class S3(config)# enable secret class
Contraseña de acceso a la consola	cisco S3#configure terminal S3(config)#line console 0 S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit
Contraseña de acceso Telnet	cisco S3#configure terminal S3(config)#line vty 0 4 S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)banner motd “Se prohibe el acceso no autorizado”

Fuente: Prueba de habilidades CCNA 2022

Paso 7: Verificar la conectividad de la red

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

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

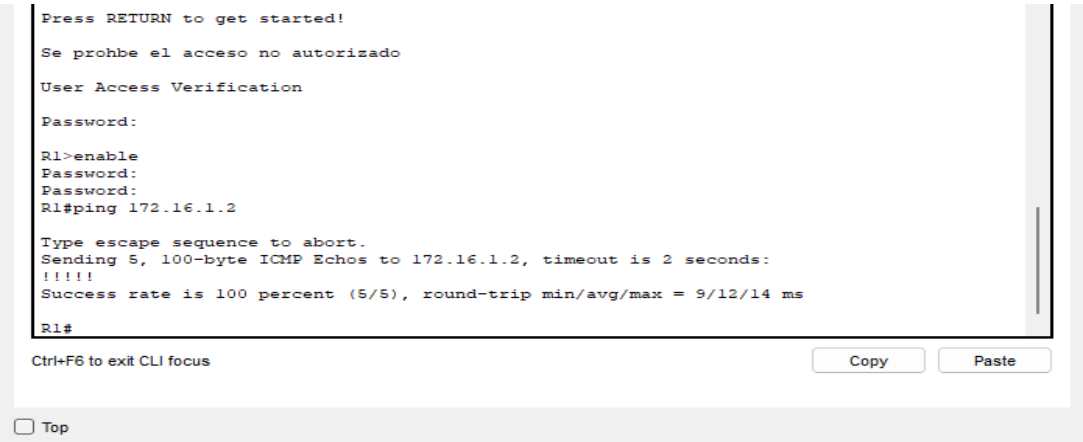
Tabla 13. Verificación de conectividad mediante ping.

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Hecho
R2	R3, S0/0/1	172.16.2.1	hecho
PC de Internet	Gateway predeterminado	209.165.200.33	hecho

Fuente: Prueba de habilidades CCNA 2022.

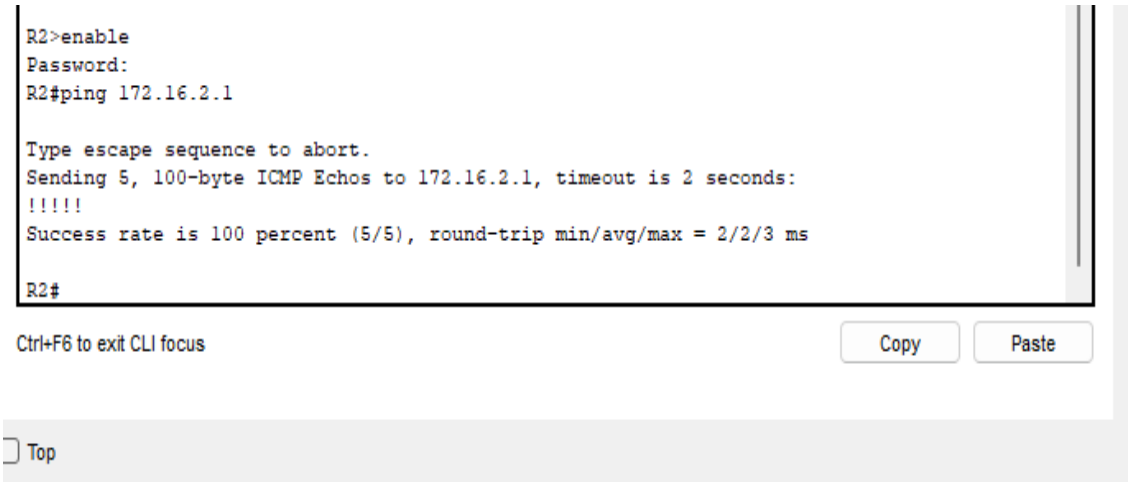
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 16. Ping del R1 al R2 escenario 2



Fuente: Propia

Figura 17. Ping del R1 al R2 escenario 2



Fuente: Propia

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

Paso 1: Configure S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración de VLAN en S1.

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config)#exit S1(config)#Vlan 23 S1(config-vlan)#name Ingenieria S1(config)#exit S1(config)#Vlan 99 S1(config-vlan)# name Administracion S1(config)#exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config)#no shutdown
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

	S1(config-if)#ip default-gateway 192.168.99.2
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#configure terminal S1(config)#interface F0/3 S1(config)# switchport mode trunk S1(config)# switchport trunk native vlan 1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#configure terminal S1(config)#interface F0/5 S1(config)# switchport mode trunk S1(config)# switchport trunk native vlan 1 S1(config)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#configure terminal S1(config-if-range)#interface range f0/1-2, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range f0/6 S1(config-range)# switchport access vlan 21 S1(config-range)#exit
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if)#shutdown

Fuente: Prueba de habilidades CCNA 2022

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración S3.

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3(config)#vlan 21 S3(config)#name Contabilidad S3(config)#exit S3(config)#Vlan 23 S3(config)#name Ingenieria S3(config)#exit S3(config)#Vlan 99 S3(config)# name Administracion S3(config)#exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#interface Vlan 99 S3(config)#ip address 192.168.99.3 255.255.255.0 S3(config)#no shutdown
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 209.165.200.225
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#configure terminal S3(config)#interface F0/3

	S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-range)# switchport mode access S3(config-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interface range f0/18 S3(config-range)# switchport access vlan 21 S3(config-range)#exit
Apagar todos los puertos sin usar	S3(config)# int range f0/1-2, f0/4-17, f0/19-24, g0/1- 2 S3(config-range)#shutdown

Fuente: Prueba de habilidades CCNA 2022

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración R1.

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.21 R1(config-subif)# description vlan 21 R1(config-subif)# encapsulation dot1q 21 R1(config-subif)# ip address 192.168.21.0 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.23 R1(config-subif)# description vlan 23 R1(config-subif)# encapsulation dot1q 23 R1(config-subif)# ip address 192.168.23.0 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración
	Asignar la VLAN 99
	Asignar la primera dirección disponible a esta interfaz
	R1(config)#interface g0/1.99
	R1(config-subif)# description vlan 99
	R1(config-subif)# encapsulation dot1q 99
	R1(config-subif)

Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shut

Fuente: Prueba de habilidades CCNA 2022

Paso 4: Verificar la conectividad de la red

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

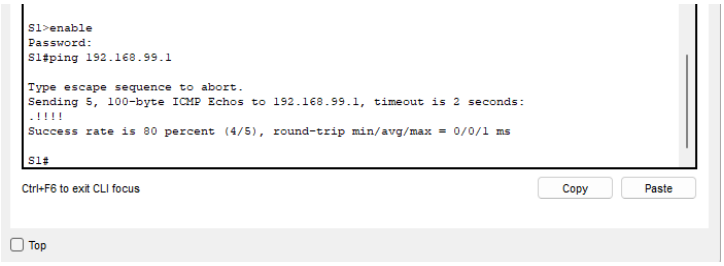
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Comprobación de conectividad.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.11	Hecho
S3	R1, dirección VLAN 99	192.168.99.1	hecho
S1	R1, dirección VLAN 21	192.168.21.1	hecho
S3	R1, dirección VLAN 23	192.168.23.1	hecho

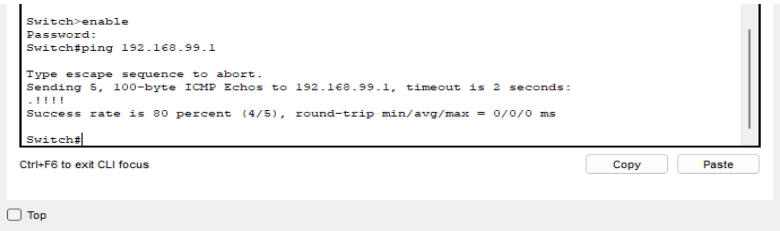
Fuente: Prueba de habilidades CCNA 2022

Figura 18. Ping desde S1 a R1, dirección VLAN 99 escenario 2.



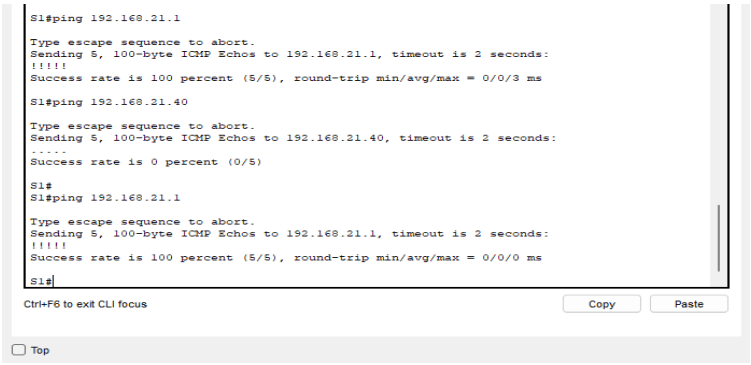
Fuente: Propia

Figura 19. Ping desde S3 a R1, dirección VLAN 99 escenario 2



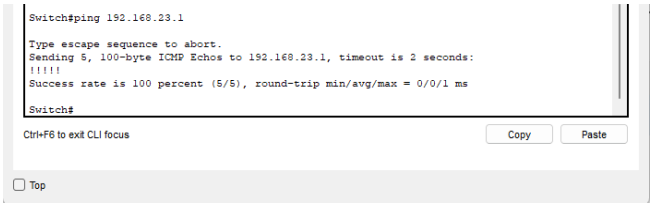
Fuente: Propia

Figura 20. Ping desde S1 a R1, dirección VLAN 21 escenario 2



Fuente: Propia

Figura 21. Ping desde S3 a R1, dirección VLAN 23 escenario 2



Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración OSFP en R1.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)# router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. #network 172.16.1.0 255.255.255.0 area 0
Establecer todas las interfaces LAN como pasivas	R1(config)#router eigrp 10 R1(config)# passive-interface g0/0 R1(config)#router eigrp 10 R1(config)# passive-interface g0/1.21 R1(config)#router eigrp 10 R1(config)# passive-interface g0/1.23 R1(config)#router eigrp 10 R1(config)# passive-interface S0/0/0 R1(config)#router eigrp 10 R1(config)# passive-interface S0/0/1
Desactive la sumarización automática	R1(config)# router rip

	R1(config-router)# no autosummary R1(config-router)# exit

Fuente: Prueba de habilidades CCNA 2022

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configuración OSFP en R2.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)# router ospf 0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#ip router ospf 0 R2(config)# passive-interface loopback0
Desactive la sumarización automática.	R2(config)# router rip R2(config-router)# no autosummary

Fuente: Prueba de habilidades CCNA 2022

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración OSFP V3 en R2.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passiveinterface loopback 4 R3(config-router)#passiveinterface loopback 5 R3(config-router)#passiveinterface loopback 6
Desactive la sumarización automática.	R3(config-router)#no autosummary

Fuente: Prueba de habilidades CCNA 2022

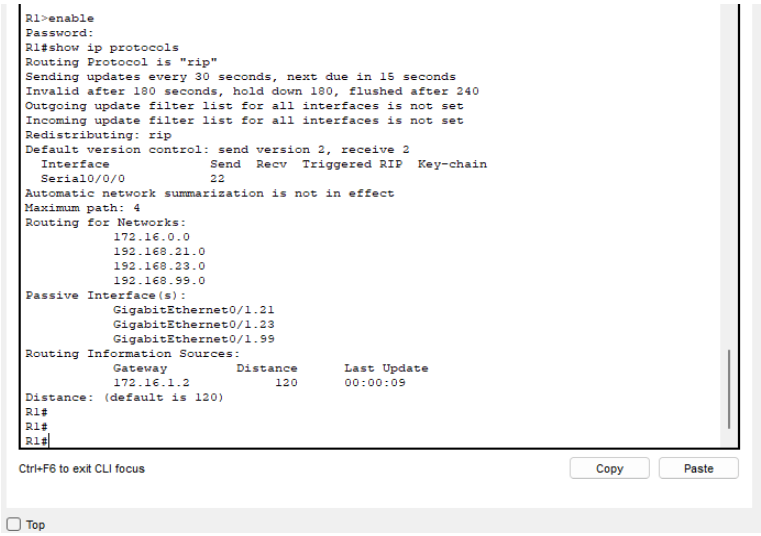
Paso 4: Verificar la información de OSPF

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

Tabla 21. Verificacion OSFP.

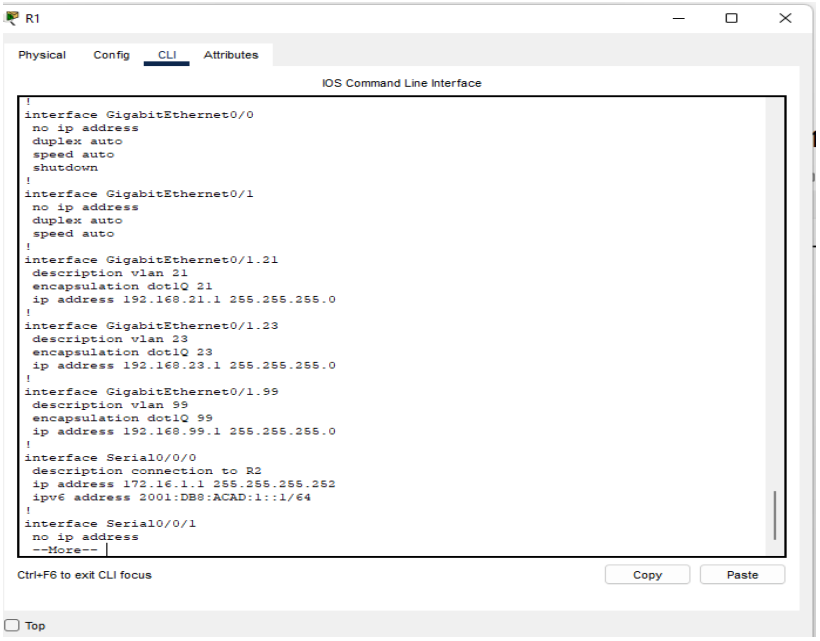
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?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

Figura 22. Ejecución de comando show ip protocols en R1 escenario 2.



Fuente: Propia

Figura 23. Ejecución de comando show run en R1 escenario 2



Fuente: Propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración DHCP y VLAN en R1.

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

	R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Fuente: Prueba de habilidades CCNA 2022

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configuración de NAT en R2.

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.237** R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0

	R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233** – **209.165.200.236** R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente: Prueba de habilidades CCNA 2022

Paso 3: Verificar el protocolo DHCP y la NAT estática

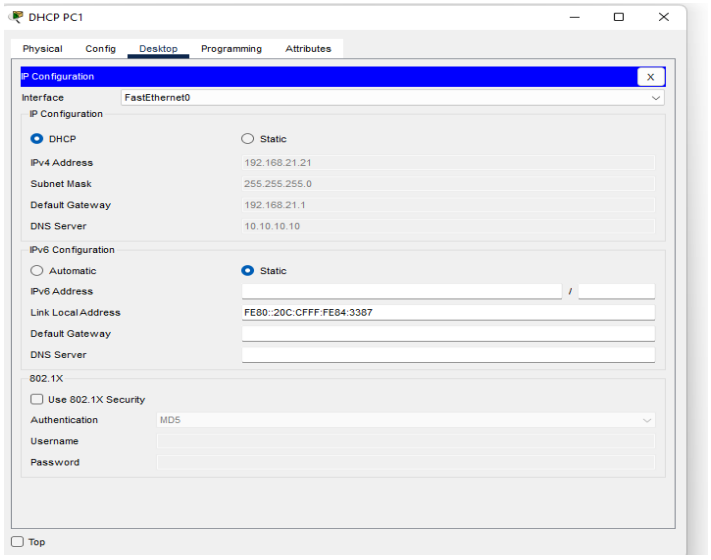
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 24. Comprobación de conectividad DHCP y NAT.

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	hecho
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	hecho
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	hecho
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**	No acepta packet tracert

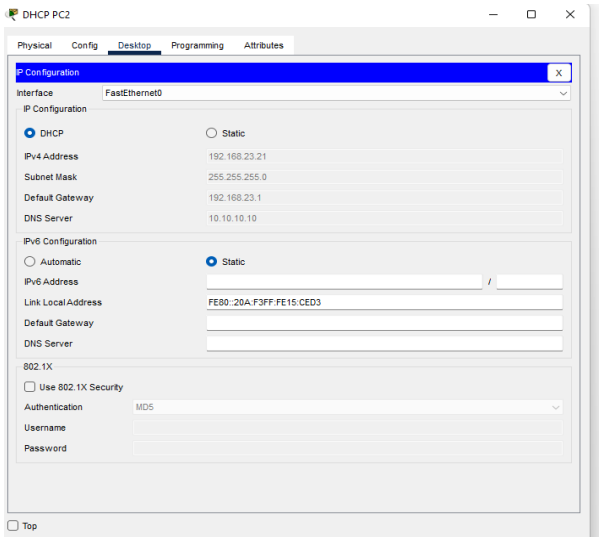
Fuente: Prueba de habilidades CCNA 2022

Figura 24. PC-A adquiere información de IP del servidor de DHCP escenario 2.



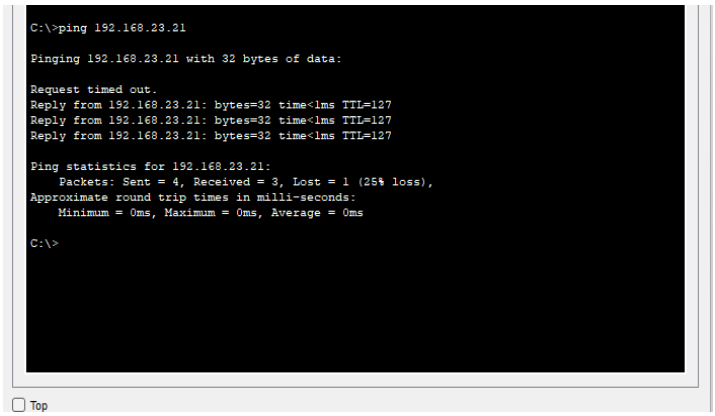
Fuente: Propia

Figura 25. PC-A adquiere información de IP del servidor de DHCP escenario 2



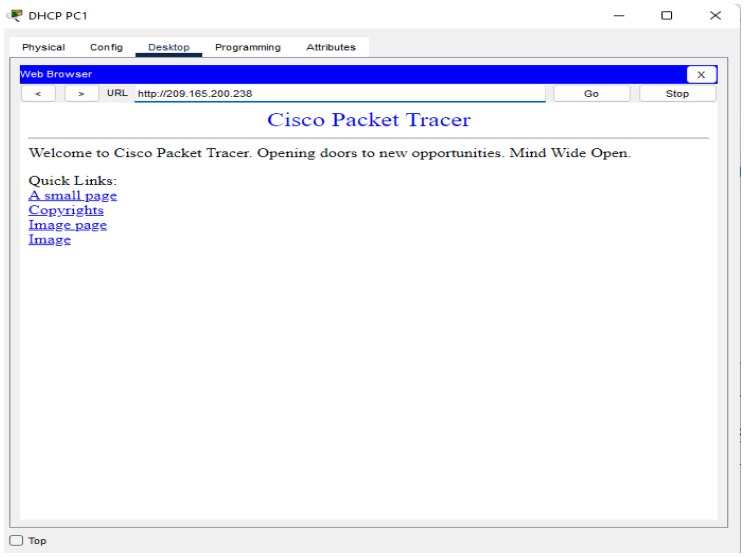
Fuente: Propia

Figura 26. PC-A ping a la PC-C escenario 2



Fuente: Propia

Figura 27. En la computadora de Internet accediendo al servidor web escenario 2



Fuente: Propia

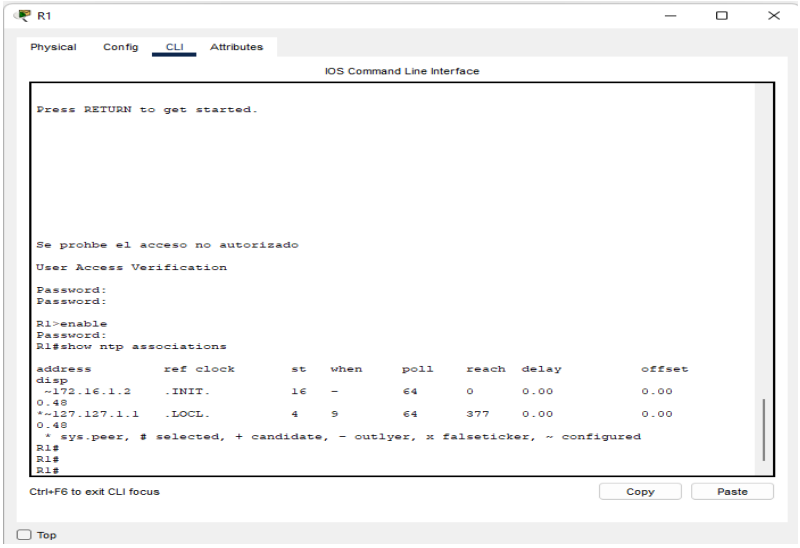
Parte 6: Configurar NTP.

Tabla 25. Configuración NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:47:00 03 may 2022
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp master 5
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp updatecalendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Fuente: Prueba de habilidades CCNA 2022

Figura 28.Verificación del comando show ntp associations en R1 escenario 2



Fuente: Propia

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

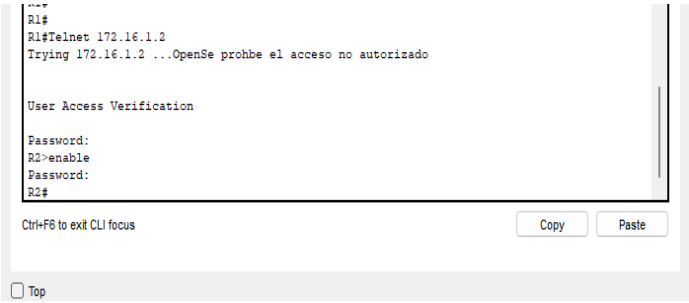
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Configuración 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	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip accesslist standard ADMINMGT R2(config-stdnacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#exit R2(config)#line vty 0 15 R2(config-line)#accessclass ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(configline)#transport input telnet
Verificar que la ACL funcione como se espera	

Fuente: Prueba de habilidades CCNA 2022

Figura 29. Verificación acceso a Telnet 172.16.1.2 escenario 2



Fuente: Propia

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

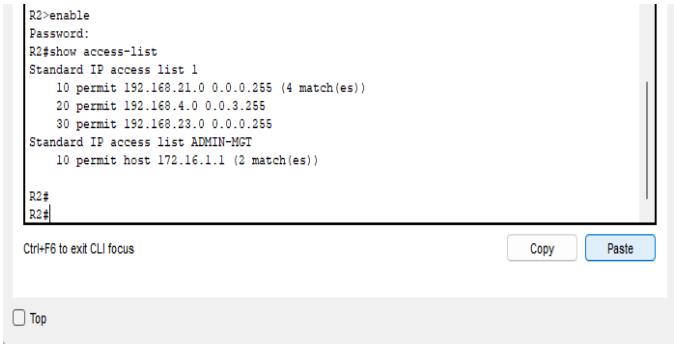
Tabla 27. Verificación de configuración.

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 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.4.0 0.0.3.255 30 permit 192.168.23.0 0.0.0.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) R2#show ip access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es))
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translations

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

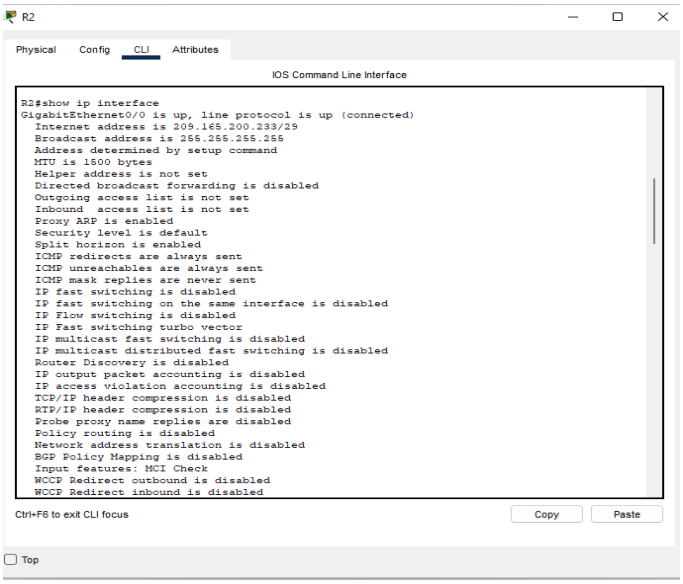
Fuente: Prueba de habilidades CCNA 2022

Figura 30. Verificación comando show access-list escenario 2



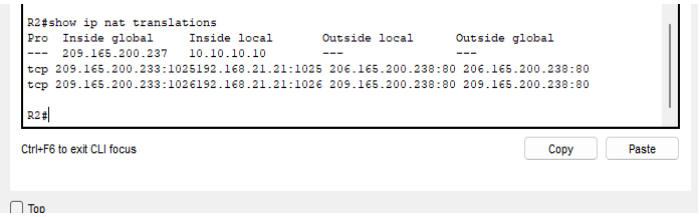
Fuente: Propia

Figura 31. Verificación comando show ip interface



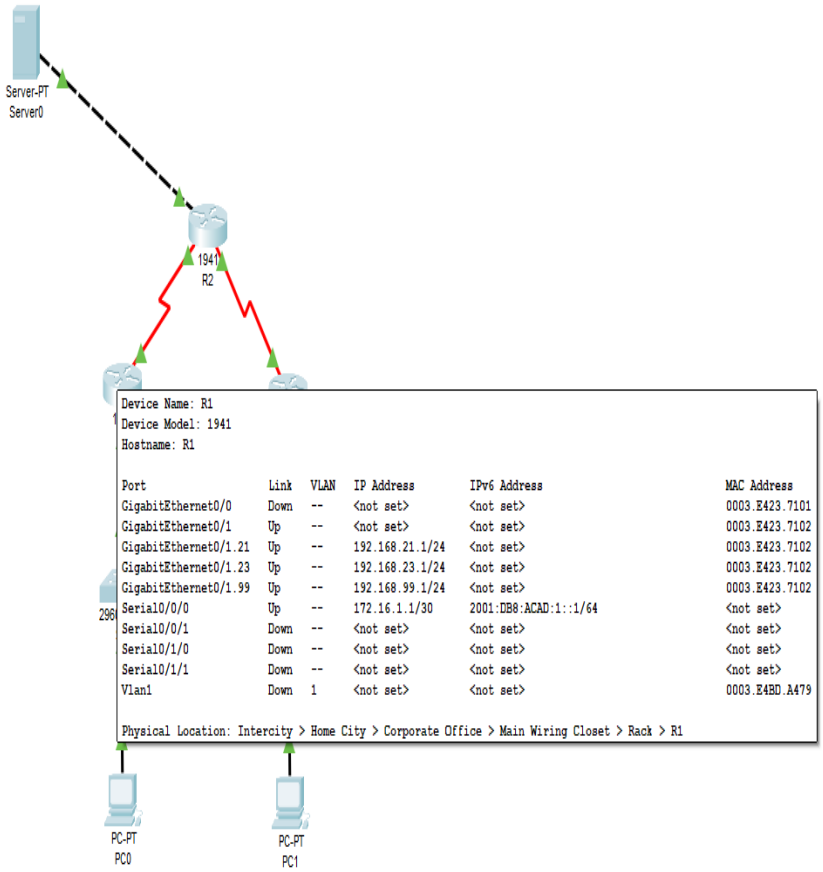
Fuente: Propia

Figura 32. Verificación del comando show ip nat translations escenario 2



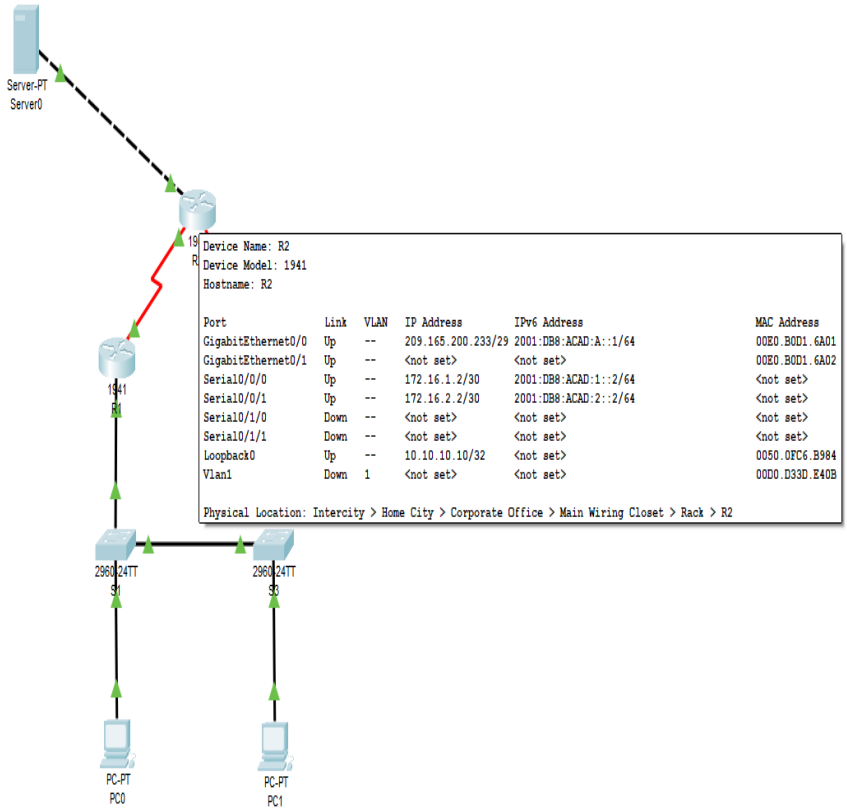
Fuente: Propia

Figura 33. Tabla de enrutamiento de R1 escenario 2



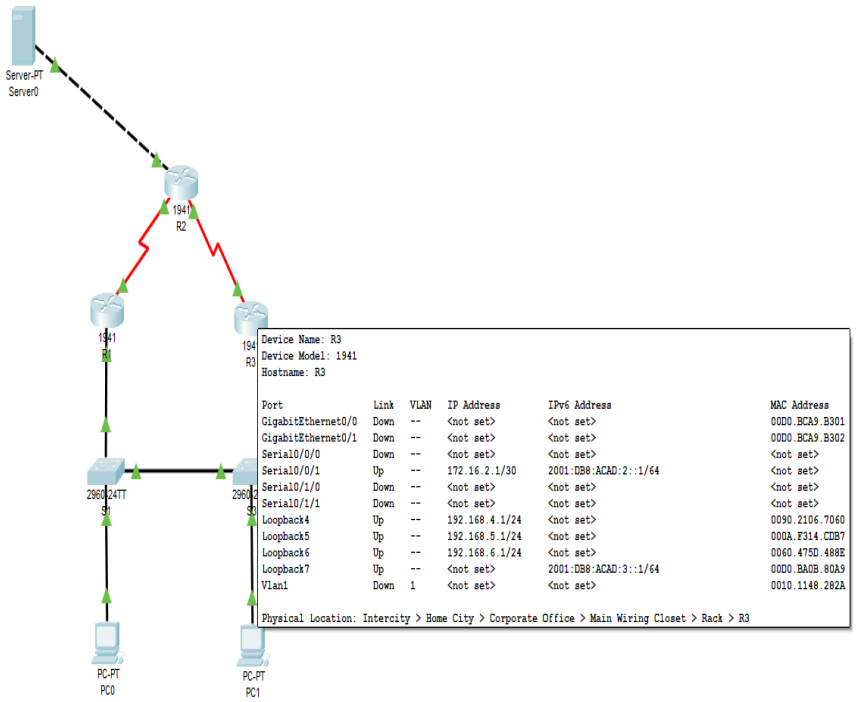
Fuente: Propia

Figura 34. Tabla de enrutamiento de R2 escenario 2



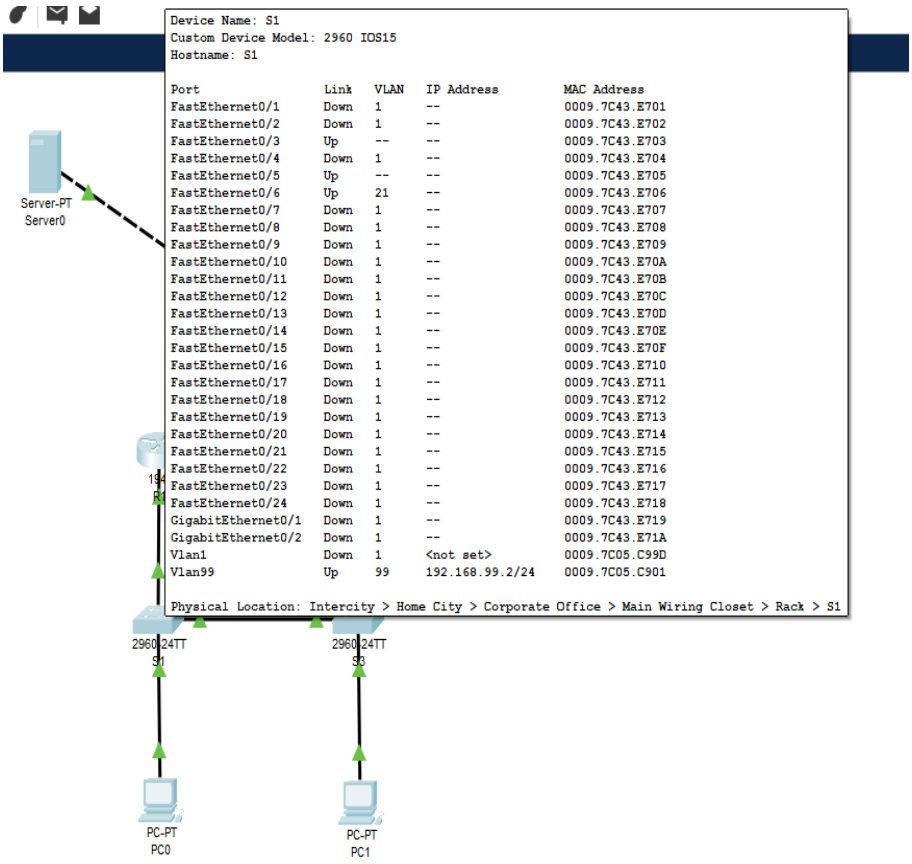
Fuente: Propia

Figura 35. Tabla de enrutamiento de R3 escenario 2



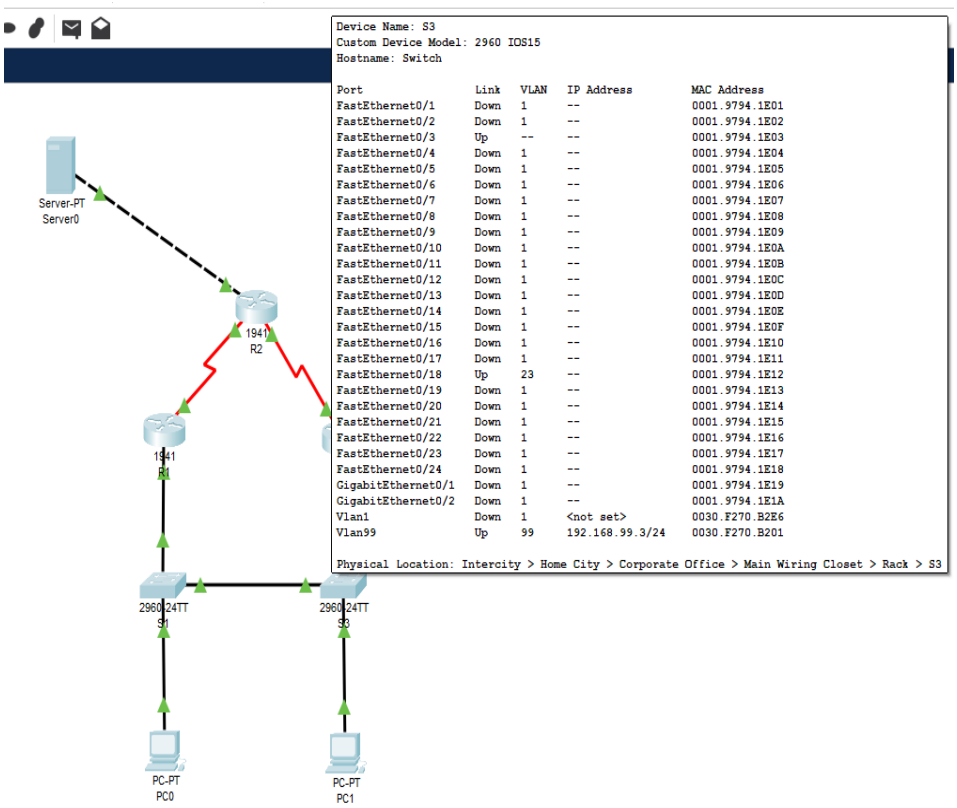
Fuente: Propia

Figura 36. Tabla de enrutamiento de S1 escenario 2



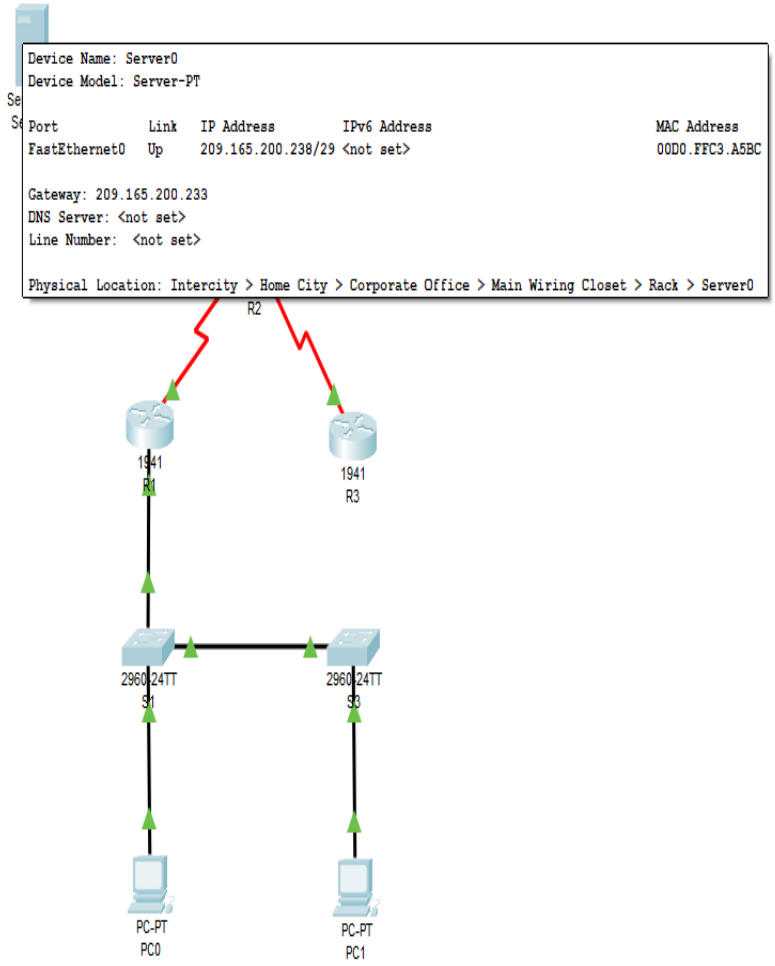
Fuente: Propia

Figura 37. escenario 2. Tabla de enrutamiento de S3



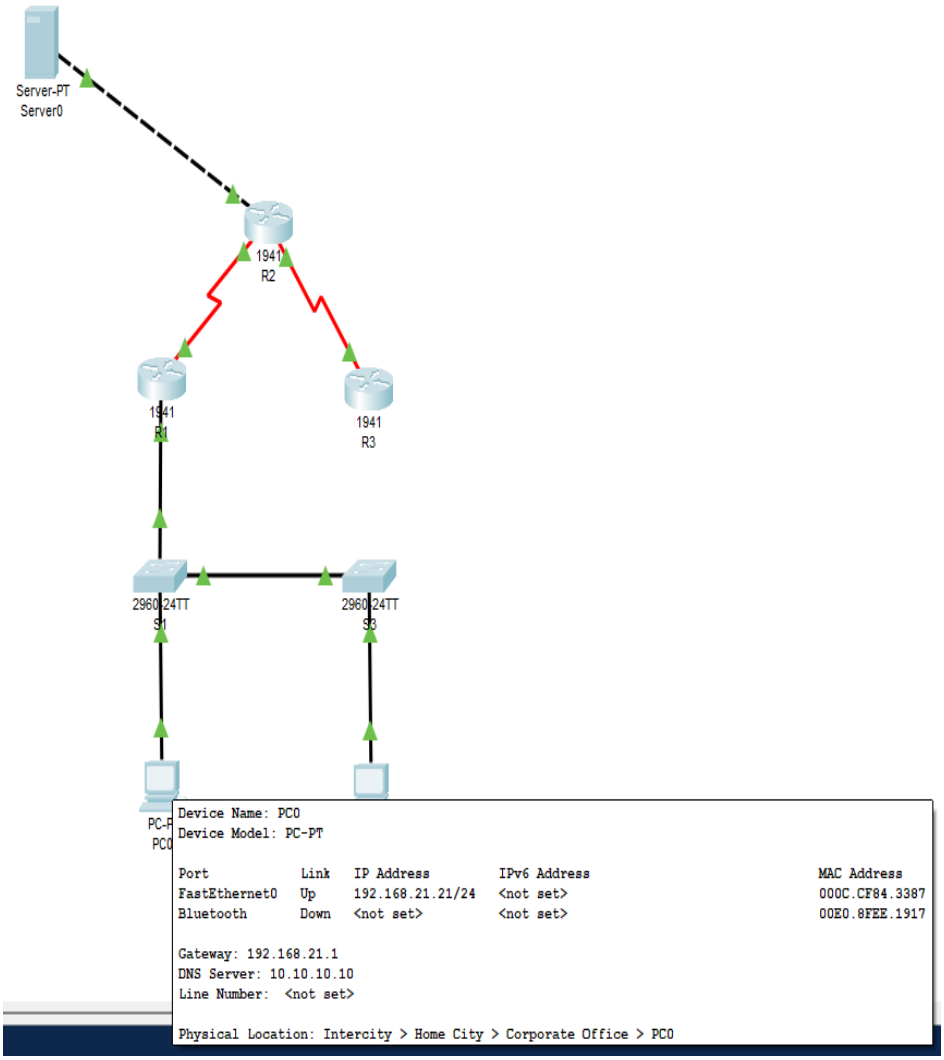
Fuente: Propia

Figura 38. Tabla de enrutamiento de server0 escenario 2



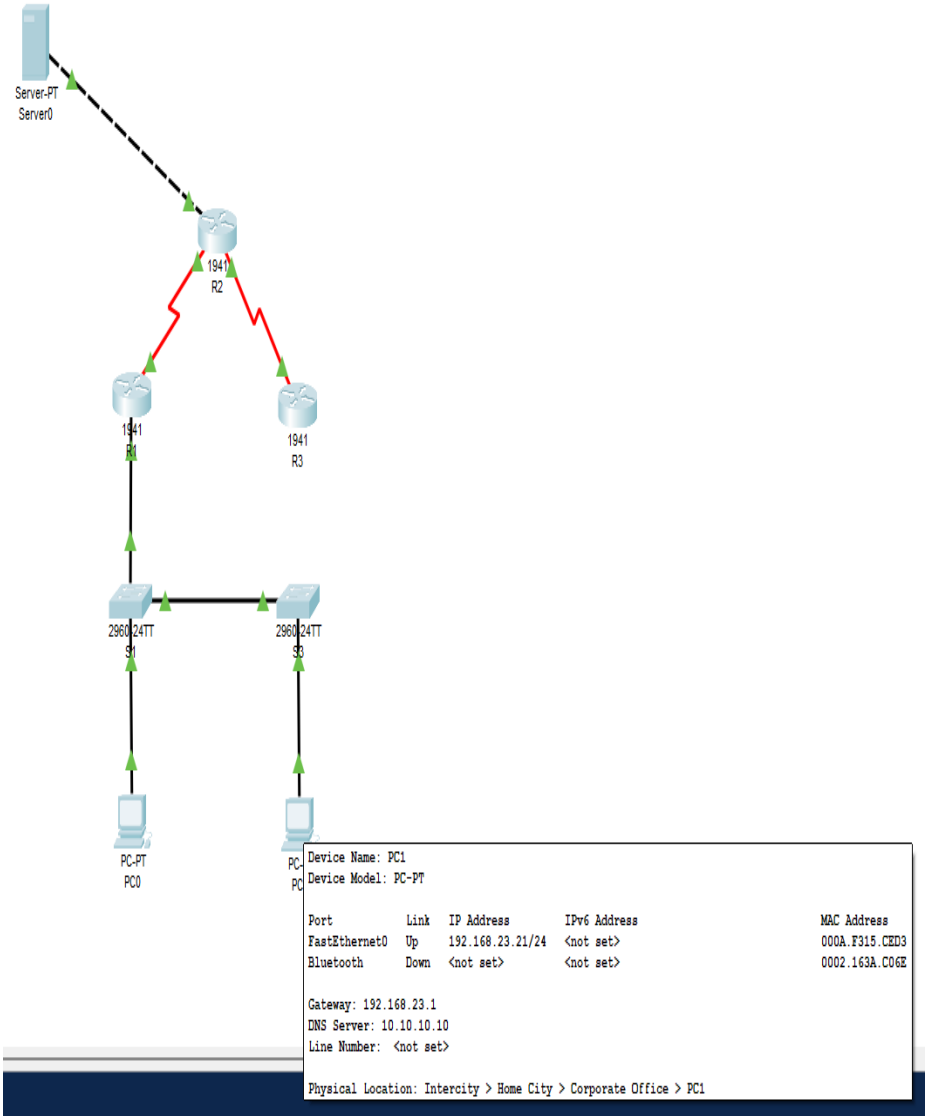
Fuente: Propia

Figura 39. Tabla de enrutamiento de PC-0 escenario 2



Fuente: Propia

Figura 40. Tabla de enrutamiento de PC-1 escenario 2



Fuente: Propia

CONCLUSIONES

Con el desarrollo de esta actividad se realizaría un numero amplio de tareas y procesos importantes para el desarrollo de los ejercicios propuestos en el trabajo final, en este se ejecutaran varias funciones como la de verificar una conexión entre los dispositivos por medio de consola ssh telnet o por un simple ping desde cada route probando las rutas ya previamente configuradas proporcionada en la configuración inicial de la topología, se configura la ACL o acceso de lista para este caso funcionaria como seguridad de configuración en la topología de los Routers, esto con el objetivo de mitigar los ataques de forma remota esto se hace por medio de un pool de direcciones no podrían faltar la verificación de la funcionalidad de las actividades ejecutadas con anterioridad.

Lo anterior esto es un poyo para el desarrollo laboral y personal de las habilidades del estudiante que está enfocado en las áreas de telecomunicaciones y telemática también es una gran opción que nos abre la universidad nacional abierta y a distancia para podernos graduar como estudiantes de ingeniería de sistemas, por eso doy profundo agradecimiento a la escuela de las ciencias básicas tecnologías de la información por el apoyo que nos da.

También en el ámbito laboral nos beneficios ya que la gran mayoría de corporaciones aun su infraestructura cuenta con tecnología cisco, aunque hay algunas como Aruba que es de HPE que trae la misma lógica que obtiene cisco de manera actual por eso es muy dispendioso aprenderse bien como es la configuración de cada equipo para cuando pasemos a la práctica no se nos sea difícil aplicarlo para una corporación.

BIBLIOGRÁFIA

CICO NETWORKING ACADEMY – CCNA 1 https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html CICO NETWORKING ACADEMY – CCNA 2 https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html Cisco CCNA – configuraicón DHCP http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-encisco-router/ Como configurar OPSF en Router http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-encisco-router/ Configuración troncal 802.1Q https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-seriesswitches/24064-171.html

CISCO. (2019). Exploración de la red. Fundamentos de Networking. https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp1.pdf

Temática: Configuración de un sistema operativo de red

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp2_.pdf

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

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

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Chp3.pdf

Temática: Acceso a la red

CISCO. (2019). Acceso a la red. Fundamentos de Networking. https://joselzapatame.webnode.com.co/_files/200000187-76fac77f50/CCNA_ITN_Chp4.pdf

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

CISCO. (2019). Ethernet. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter5_Ethernet.pdf

Temática: Capa de red

CISCO. (2019). Capa de red. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter6_Capa%20de%20red.pdf CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter9_Divisi%c3%b3n%20de%20redes%20IP%20en%20subredes.pdf

CISCO. (2019). Capa de transporte. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter7_Capa%20de%20transporte.pdf

Temática: Capa de aplicación

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter10_Capa%20de%20aplicacion.pdf

Temática: Configuración de un sistema operativo de red

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter11_Es%20una%20red.pdf

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/01_Routing_Concept.pdf

Temática: Routing Estático

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/02_Static_Routing.pdf

OVA Unidad 6 - Configuración de Switches y Routers

Este Objeto Virtual de Aprendizaje, titulado Vídeo - Configuración de Switches y Routers, tiene como objetivo, orientar al estudiante sobre los comando básicos del IOS para la configuración de equipos de conmutación y enrutamiento.

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

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/03_Dynamic_Routing.pdf

Temática:Redes Conmutadas

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/04_Switched_Networks.pdf

OVA Unidad 7 - Principios de Enrutamiento.

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

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/05_Switch_Configuration.pdf

Temática:VLAN

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/06_VLANs.pdf

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. http://www.ie.tec.ac.cr/einteriano/cisco/ccna4/Presentaciones/CCNA_Exploration_Accessing_the_WAN_-_Cap5.pdf

Temática: DHCP

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/08_DHCP.pdf

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/09_NAT_for_IPv4.pdf

Temática: Detección, Administración y Mantenimiento de Dispositivos

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/10_Discover_Manage_Maintenance.pdf