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

NICOLAS GARCIA BONILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

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

NICOLAS GARCÍA BONILLA

Diplomado de opción de grado para optar por el título de
INGENIERO DE SISTEMAS

DIRECTOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
IBAGUÉ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

IBAGUÉ, 30 de noviembre 2020

AGRADECIMIENTOS

En primera instancia agradecer a mi familia y circulo social por su inagotable apoyo en este arduo camino de formación como ingeniero. A la Universidad Nacional Abierta y a Distancia – UNAD por haberme brindado la oportunidad de ingresar a ser parte de tan importante institución y cursar mi ingeniería allí. Al grupo de tutores y compañeros de estudio que me brindaron todo el acompañamiento necesario en el desarrollo de todos y cada uno de los cursos de la carrera universitaria.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Banda ancha: Se refiere a la transmisión de datos en la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión.

DHCP (Dynamic Host Configuration Protocol): Protocolo destinado a la obtención de una dirección IP para nuestra conexión de manera aleatoria, en lugar de disponer permanentemente de una única dirección.

DNS (Domain Name System): Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP, por ejemplo de: www.asesoriainformatica.com a: 200.57.147.12.

Firewall: Programa o equipo que separa a un equipo, una red local (LAN) o una red global (WAN) en dos o más partes, con propósitos de seguridad, limitando o supervisando los accesos a sus recursos.

Gateway: Programa o equipo que se encarga de traducir la información contenida en dos
protocolos diferentes.

HTTP (Hipertext Transfer Protocol): Protocolo de transferencia de hipertexto. Conjunto de estándares que permite a los usuarios de la Web intercambiar información. Método que se utiliza para transferir documentos desde el sistema donde se almacenan las páginas hasta los usuarios individuales.

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

Protocolo: Conjunto de reglas y normas que determinan cómo se realiza un intercambio de datos, asegurando que los datos recibidos son idénticos a los datos enviados.

RESUMEN

Dentro del desarrollo del diplomado de profundización cisco se plantean dos escenarios los cuales se llevan a cabo basándose en una serie de topologías y configuraciones de diferentes dispositivos de red, que están diseñadas para evaluar y poner en práctica los conocimientos en networking que se han adquirido durante el desarrollo del diplomado. Se emplea el uso del Software Cisco Packet Tracer para realizar las simulaciones de los ejercicios propuestos para así lograr cumplir a cabalidad con los requerimientos propuestos en las configuraciones de las redes planteadas.

PALABRAS CLAVE: Escenario, Topología, Interfaz, Router, Switch, Servidor, Internet.

ABSTRACT

Within the development of the Cisco in-depth diploma course, two scenarios are proposed, which are carried out based on a series of topologies and configurations of different network devices, which are designed to evaluate and put into practice the networking knowledge that has been acquired during the development of the diploma. The use of Cisco Packet Tracer Software is used to perform the simulations of the proposed exercises in order to fully comply with the requirements proposed in the proposed network configurations.

KEY WORDS: Scenario, Topology, Interface, Router, Switch, Server, Internet.

INTRODUCCIÓN

Actualmente las telecomunicaciones son consideradas de gran importancia en el diario vivir de las personas a lo largo del mundo. Gracias a la implementación de estas tecnologías se fomenta el desarrollo socioeconómico de las poblaciones, hay desarrollo empresarial, el sector salud mejora sus servicios, la educación se vuelve más practica y de fácil acceso, entre muchos otros beneficios que mencionar.

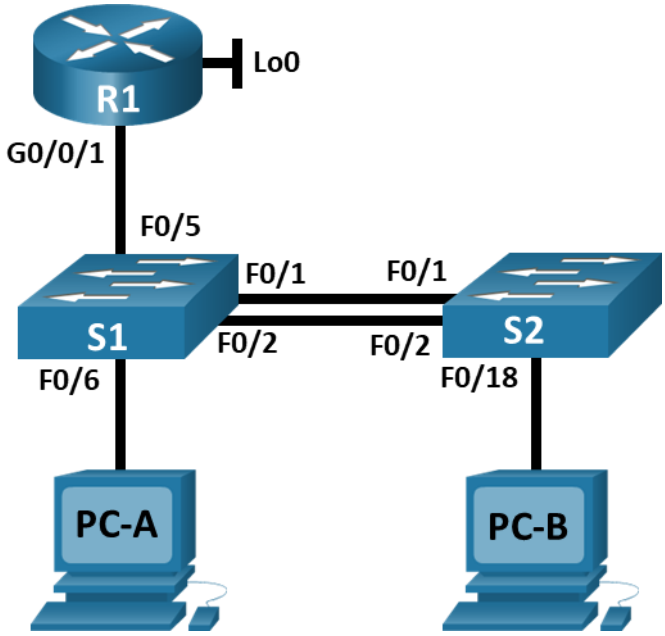
Por lo anterior se hace necesario que los profesionales en este campo estén a plena capacidad de llevar a cabo proyectos e integraciones empleando este tipo de tecnologías haciendo uso de las buenas prácticas de configuración y seguridad permitiendo tener un control y gestión de los servicios de TI.

En el contenido del presente documento se denota de manera detallada el procedimiento para implementar dos redes propuestas en los escenarios que incluyen configuración básica de dispositivos de red, direccionamiento IPv4 e IPv6, routing, configuración de Vlan, EtherChannel, servicios DHCP, NAT, ACL, NTP y routing OSPFv2 y OSPFv3. Para la consecución de lo anterior fue necesario poner en práctica, profundizar e investigar en los conocimientos, técnicas, habilidades y competencias adquiridas durante el desarrollo del Diplomado.

DESARROLLO DEL PROYECTO

Escenario 1

Figura 1. Topología Escenario 1.



Fuente: Repositorio UNAD.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1. Tabla de VLAN.

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 2. Tabla de asignación de direcciones.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

Instrucciones

Inicializar y Recargar y Configurar aspectos basicos de los dispositivos.

Inicializar y volver a cargar el router y el switch.

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

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

Tabla 3. Instrucciones y comandos de configuración para inicializar y volver a cargar los dispositivos de la red.

Tarea	Especificación
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

Tabla 4. Configuración de la plantilla SDM en Switch S1 y S2.

Tarea	Especificación
Configurar la plantella SDM	sdm prefer dual-ipv4-and-ipv6 default
Volver a cargar el dispositivo	reload

Como parte inicial se elimina cualquier tipo de configuración inicial presente en los routers y switches. Se borra la tabla de vlan de los conmutadores y se recargan todos los dispositivos para aplicar los cambios.

Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

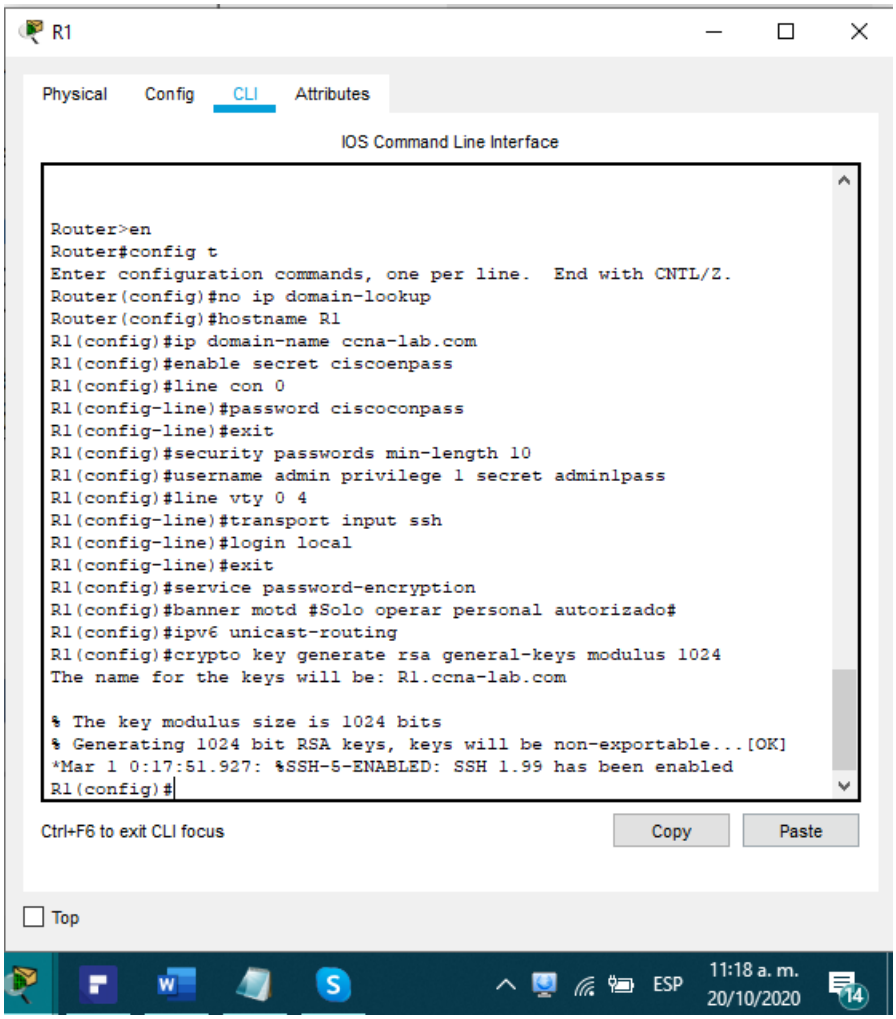
Tabla 5. Instrucciones y comandos para configuración básica y de interfaces en R1.

Tarea	Especificación
Desactivar la búsqueda DNS	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 secret ciscoenpass

Contraseña de acceso a la consola	line con 0 password ciscoconpass exit
Establecer la longitud mínima para las contraseñas	security passwords min-length 10
Crear un usuario administrativo en la base de datos local	username admin privilege 1 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 4 login local exit
Configurar VTY solo aceptando SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configure un MOTD Banner	banner motd #Solo operar personal autorizado#
Habilitar el routing IPv6	ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	int gi0/1 description LAN R1,S1 int gi0/1.2 description Bikes encapsulation dot1q 2 ip address 10.19.8.1 255.255.255.192 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:a::1/64 exit int gi0/1.3 description Trikes encapsulation dot1q 3 ip address 10.19.8.65 255.255.255.224 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:b::1/64 exit int gi0/1.4 description Management encapsulation dot1q 4 ip address 10.19.8.97 255.255.255.248 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:c::1/64 exit int gi0/1 no shutdown exit

Configure el Loopback0 interface	int loopback0 description LOOPBACK ip address 209.165.201.1 255.255.255.224 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:209::1/64 exit
Generar una clave de cifrado RSA	crypto key generate rsa general-keys modulus 1024

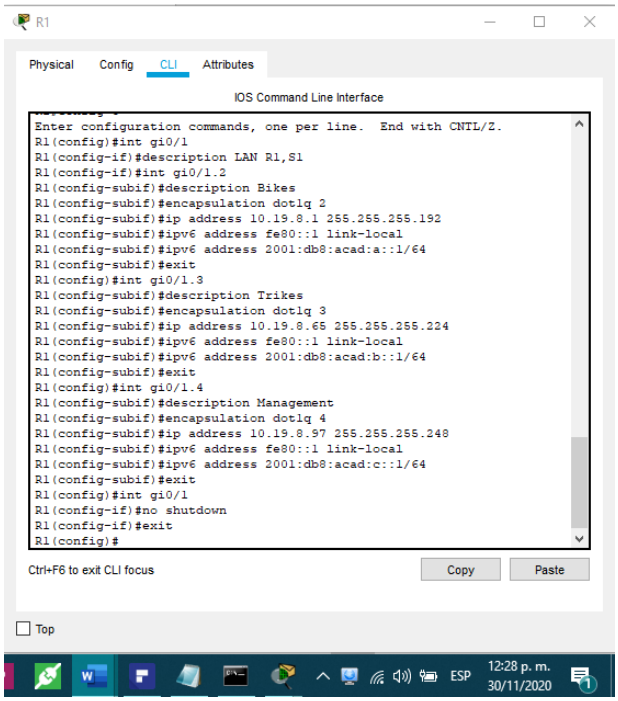
Figura 2. Configuración de parámetros básicos Router R1.



Fuente: Autor.

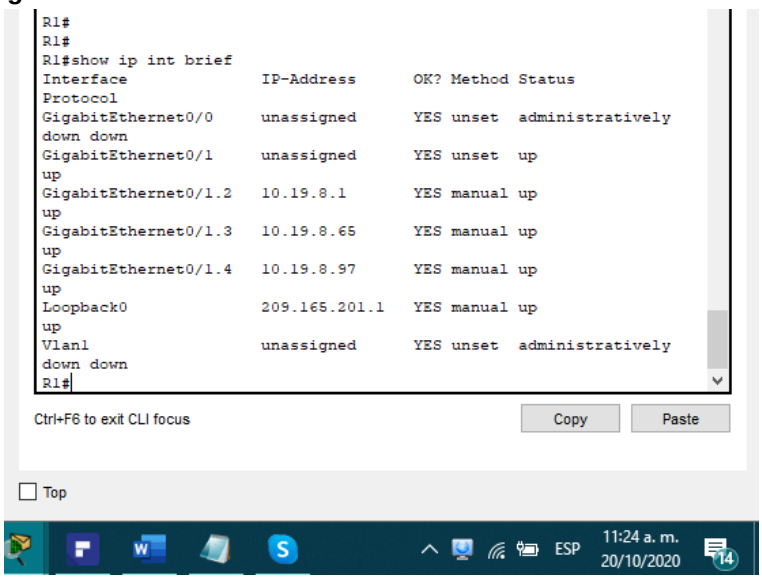
Se establece la configuración inicial para R1. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados.

Figura 3. Configuración de interfaces (descripción, IPv4, IPv6) en R1.



Fuente: Autor.

Figura 4. Estado general de las interfaces de Router R1.



Fuente: Autor.

Se configuran las interfaces y subinterfaces de R1 estableciendo su descripción y su direccionamiento IP. Se verifica el estado de las mismas empleando el comando "show ip int brief".

Configure S1 y S2.

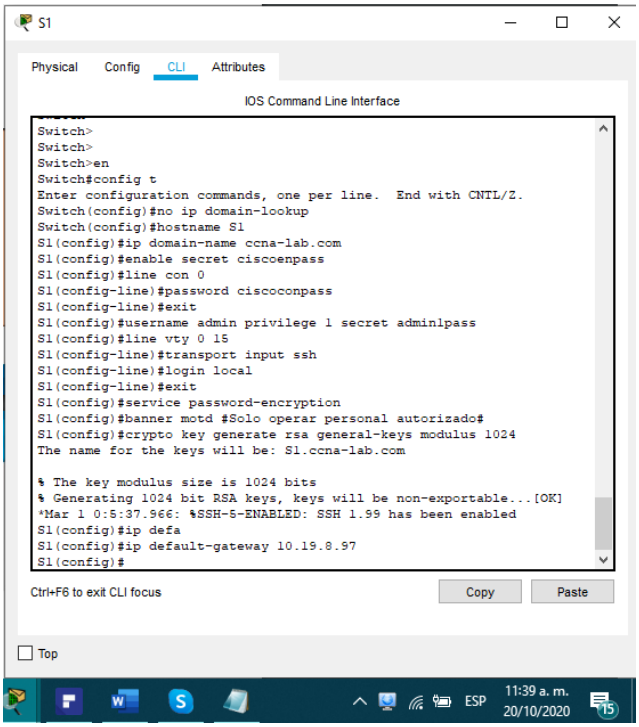
Las tareas de configuración incluyen lo siguiente:

Tabla 6. Instrucciones y comandos para configuración básica y de interfaces en S1 y S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	no ip domain-lookup
Nombre del switch	hostname S1 o S2
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	enable secret ciscoenpass
Contraseña de acceso a la consola	line con 0 password ciscoconpass exit
Crear un usuario administrativo en la base de datos local	username admin privilege 1 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local exit

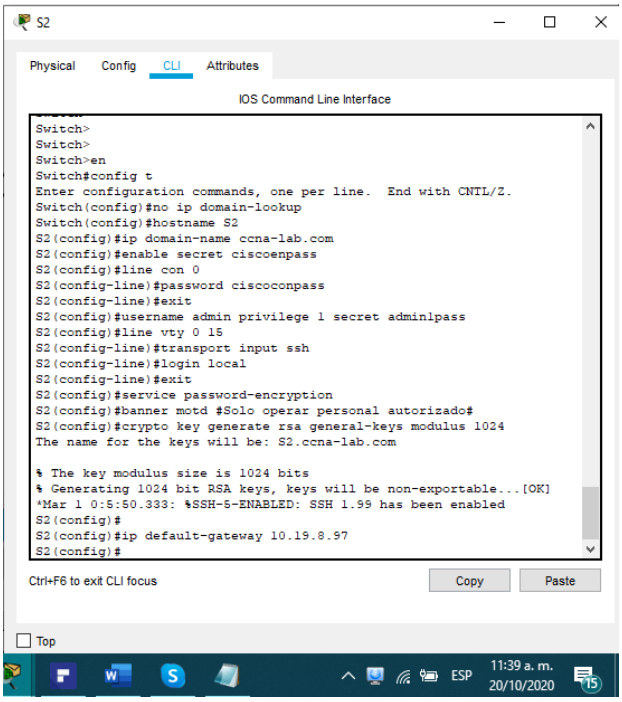
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configurar un MOTD Banner	banner motd #Solo operar personal autorizado#
Generar una clave de cifrado RSA	crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Vlan 4 name Management exit int Vlan 4 ip address 10.19.8.98 255.255.255.248 ipv6 address fe80::98 link-local ipv6 address 2001:db8:acad:c::98/64 exit
Configuración del gateway predeterminado	ip default-gateway 10.19.8.97

Figura 5. Configuración de parámetros básicos en Switch S1.



Fuente: Autor.

Figura 6. Configuración de parámetros básicos en Switch S2.



Fuente: Autor.

Se establece la configuración inicial para S1 y S2. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados.

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Configurar S1

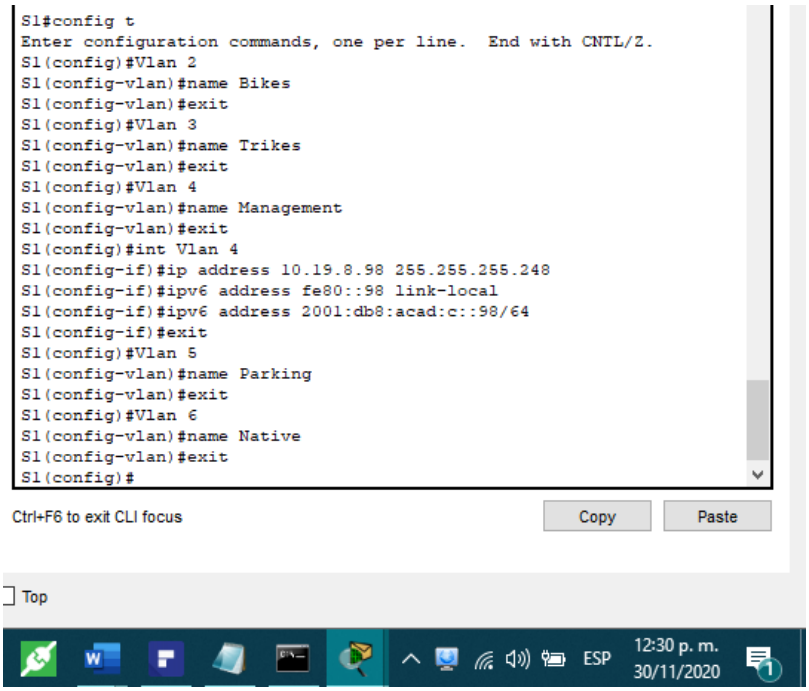
La configuración del S1 incluye las siguientes tareas:

Tabla 7. Instrucciones y comandos de configuración de la estructura de red en S1.

Tarea	Especificación
Crear VLAN	Vlan 2 name Bikes exit Vlan 3 name Trikes exit Vlan 4 name Management exit int Vlan 4 ip address 10.19.8.98 255.255.255.248 ipv6 address fe80::98 link-local ipv6 address 2001:db8:acad:c::98/64 exit Vlan 5 name Parking exit Vlan 6 name Native exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	int f0/1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/2

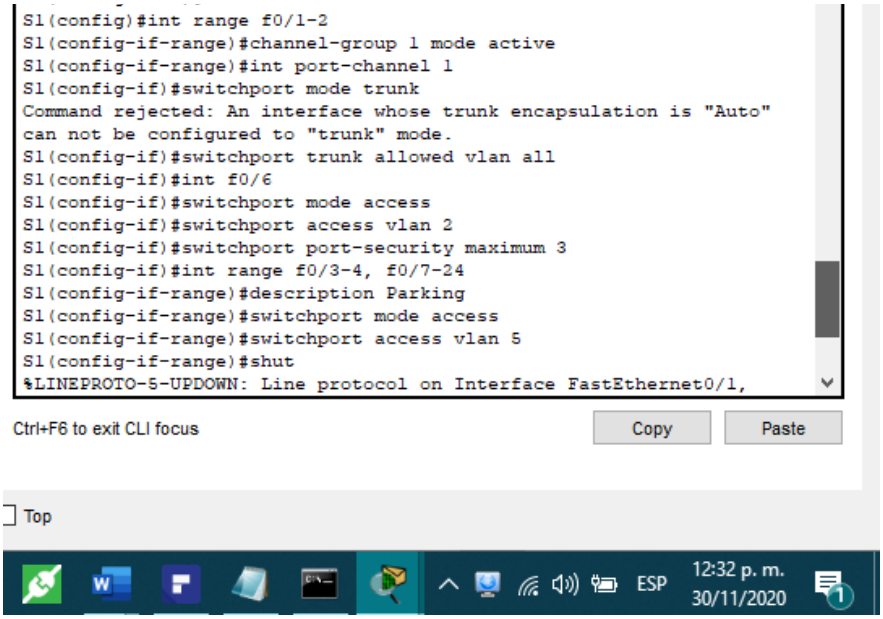
	switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/5 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	int range f0/1-2 channel-group 1 mode active int port-channel 1 switchport mode trunk switchport trunk allowed vlan all
Configurar el puerto de acceso de host para VLAN 2	int f0/6 switchport mode access switchport access vlan 2 end
Configurar la seguridad del puerto en los puertos de acceso	switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	int range f0/3-4, f0/7-24 description Parking switchport mode access switchport access vlan 5 shut end

Figura 7. Creación de VLAN en S1.



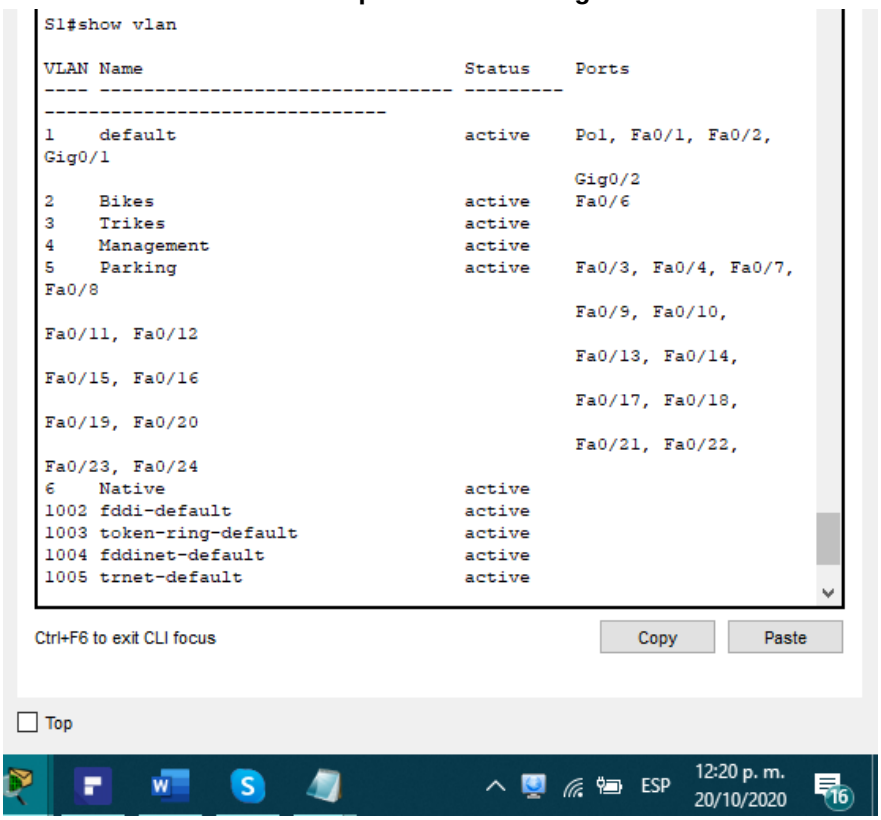
Fuente: Autor.

Figura 8. Configuración de interfaces en S1.



Fuente: Autor.

Figura 9. Estado de las Vlan's en S1 después de las configuraciones realizadas.



Fuente: Autor.

Se crean las VLAN en S1 con su respectivo nombre y direccionamiento IP. Se establecen los enlaces troncales y los grupos de puertos EtherChannel en las interfaces indicadas. Se configura la seguridad y protección de las demás interfaces. Con el comando "show vlan" verificamos el estado general de las Vlan en S1.

Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

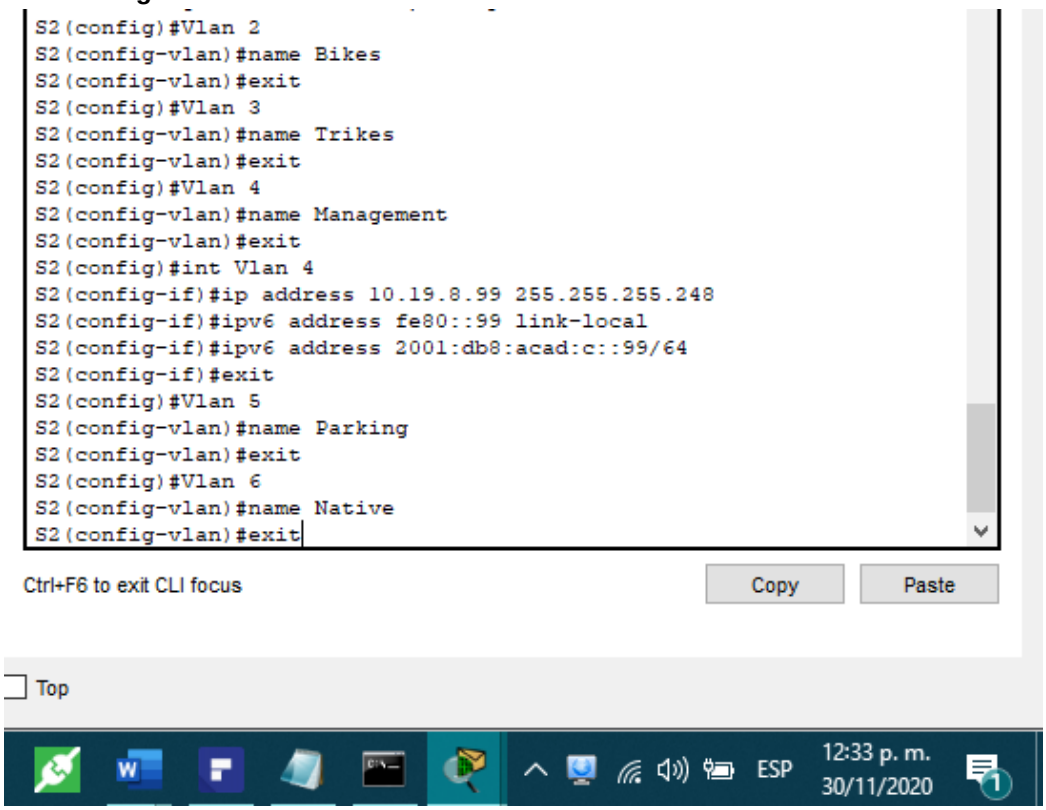
Tabla 8. Instrucciones y comandos de configuración de la estructura de red en S2.

Tarea	Especificación
Crear VLAN	Vlan 2 name Bikes exit Vlan 3 name Trikes exit Vlan 4

	name Management exit int Vlan 4 ip address 10.19.8.99 255.255.255.248 ipv6 address fe80::99 link-local ipv6 address 2001:db8:acad:c::99/64 exit Vlan 5 name Parking exit Vlan 6 name Native exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	int f0/1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/5 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	int range f0/1-2 channel-group 1 mode active int port-channel 1 switchport mode trunk switchport trunk allowed vlan all end
Configurar el puerto de acceso del host para la VLAN 3	int f0/18 switchport mode access switchport access vlan 3 end

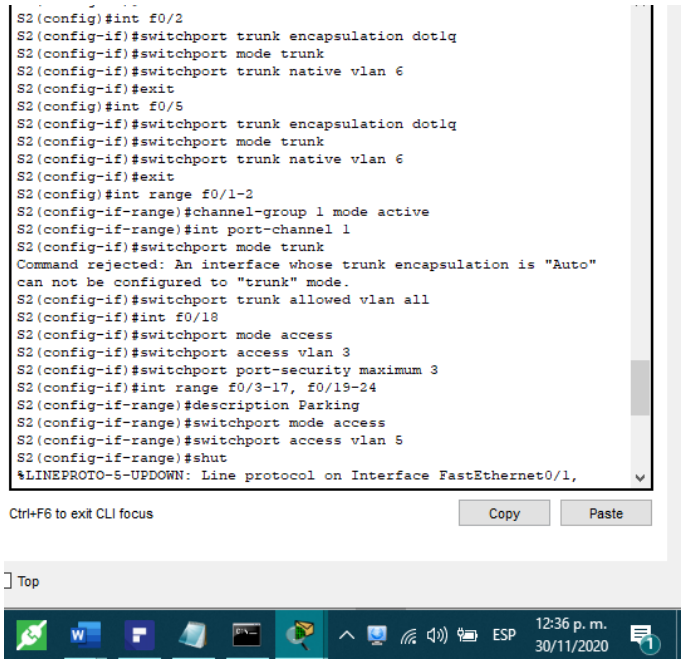
Configure port-security en los access ports	switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	int range f0/3-17, f0/19-24 description Parking switchport mode access switchport access vlan 5 shut end

Figura 10. Configuración de VLAN en S2.



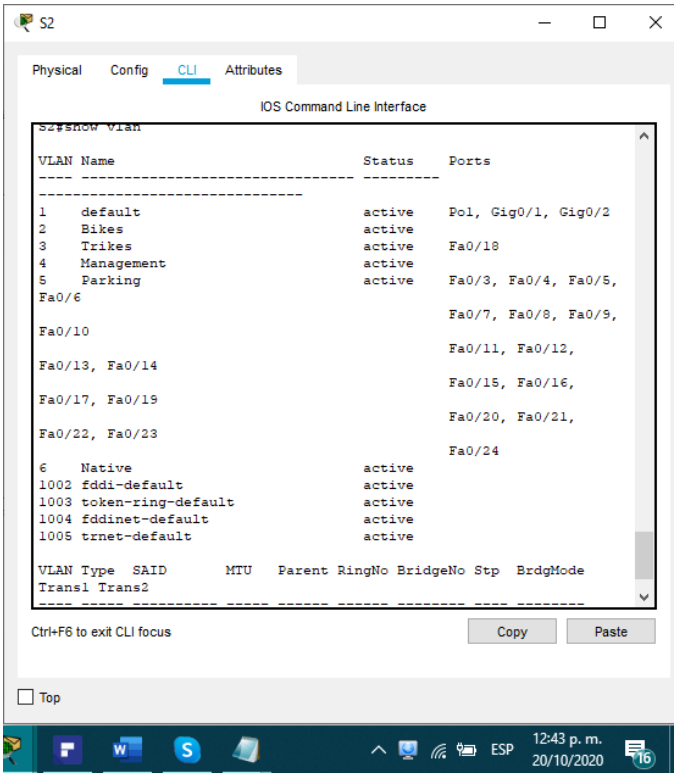
Fuente: Autor.

Figura 11. Configuración de interfaces en S2.



Fuente: Autor.

Figura 12. Estado de las Vlan's en S2 después de las configuraciones realizadas.



Fuente: Autor.

Se crean las VLAN en S2 con su respectivo nombre y direccionamiento IP. Se establecen los enlaces troncales y los grupos de puertos EtherChannel en las interfaces indicadas. Se configura la seguridad y protección de las demás interfaces. Con el comando "show vlan" verificamos el estado general de las Vlan en S2.

Configurar soporte de host

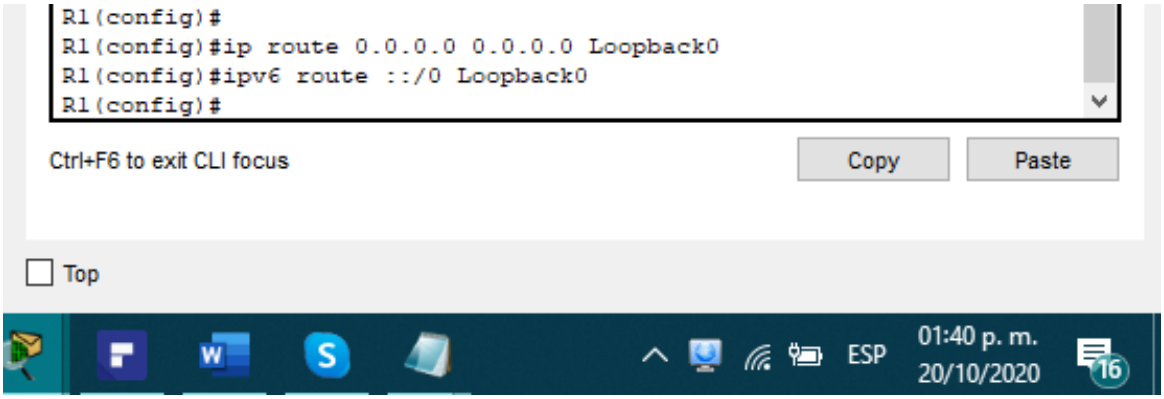
Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Instrucciones y comandos de configuración para soporte de host en R1.

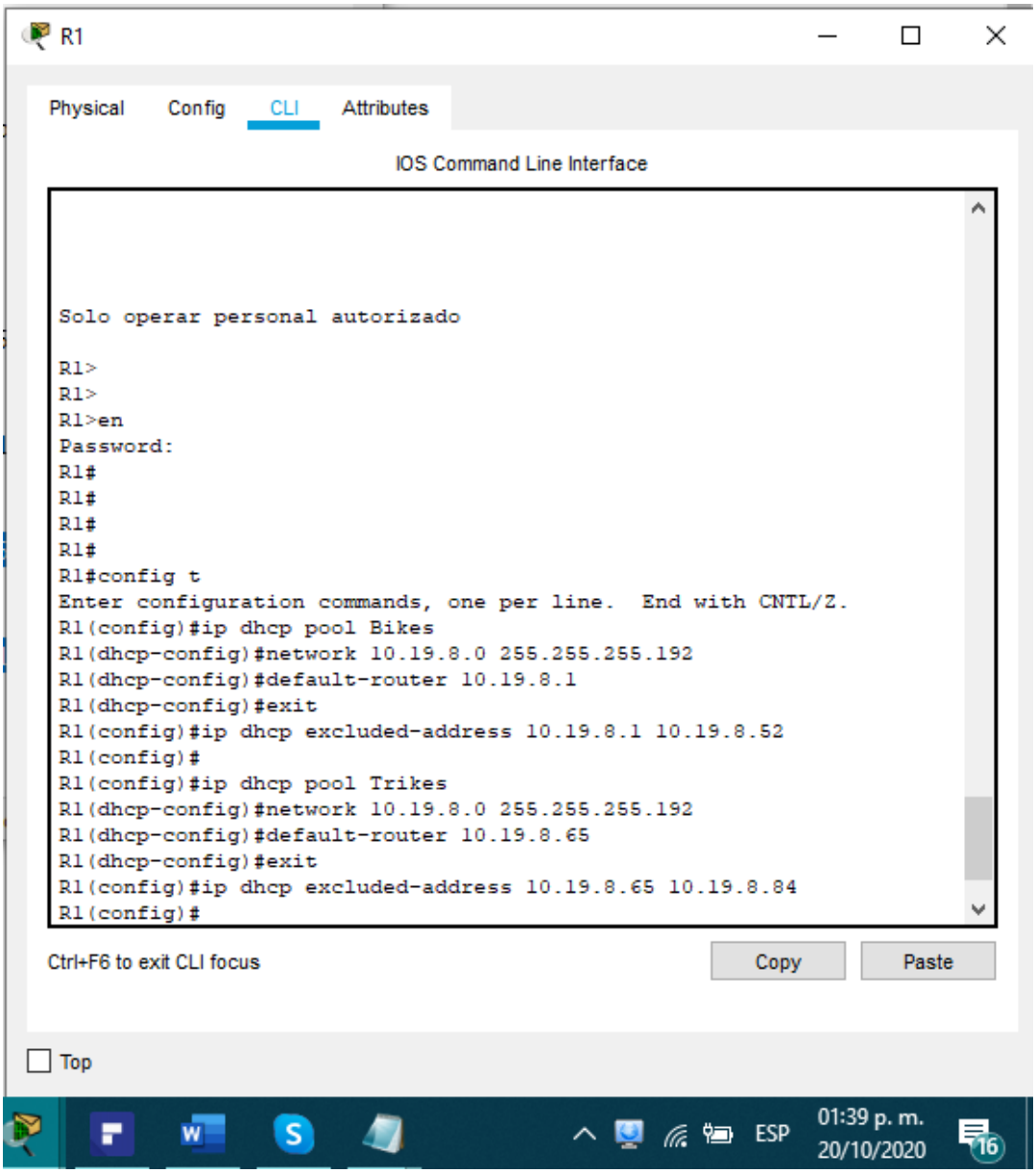
Tarea	Especificación
Configure Default Routing	ip route 0.0.0.0 0.0.0.0 Loopback0 ipv6 route ::/0 Loopback0
Configurar IPv4 DHCP para VLAN 2	ip dhcp pool Bikes network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 exit ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	ip dhcp pool Trikes network 10.19.8.64 255.255.255.224 default-router 10.19.8.65 exit ip dhcp excluded-address 10.19.8.65 10.19.8.84

Figura 13. Comandos empleados para la creación de las rutas predeterminadas.



Fuente: Autor.

Figura 14. Comandos ejecutados para la creación de los grupos DHCP para las Vlan 2 y 3.



Fuente: Autor.

Configuramos la ruta predeterminada para la interfaz Loopback0 y el servicio DHCP para las Vlan 2 y 3 en R1 excluyendo el grupo de direcciones IP planteados para cada Vlan.

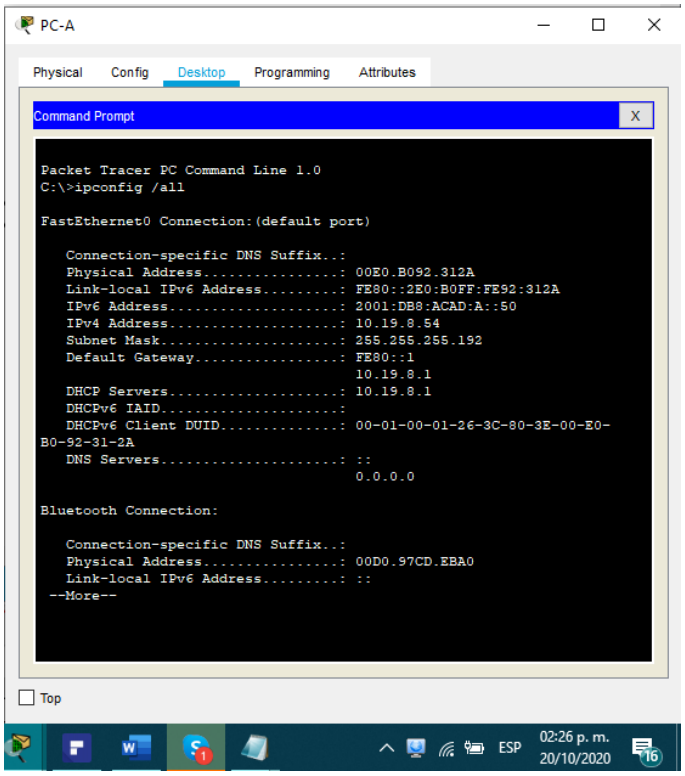
Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 10. Configuración de red en PC-A.

PC-A Network Configuration	
Descripción	FastEthernet0
Dirección física	00E0:B092:312A
Dirección IP	10.19.8.54 2001:DB8:ACAD:A::50
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 15. Configuración de red de PC-A.



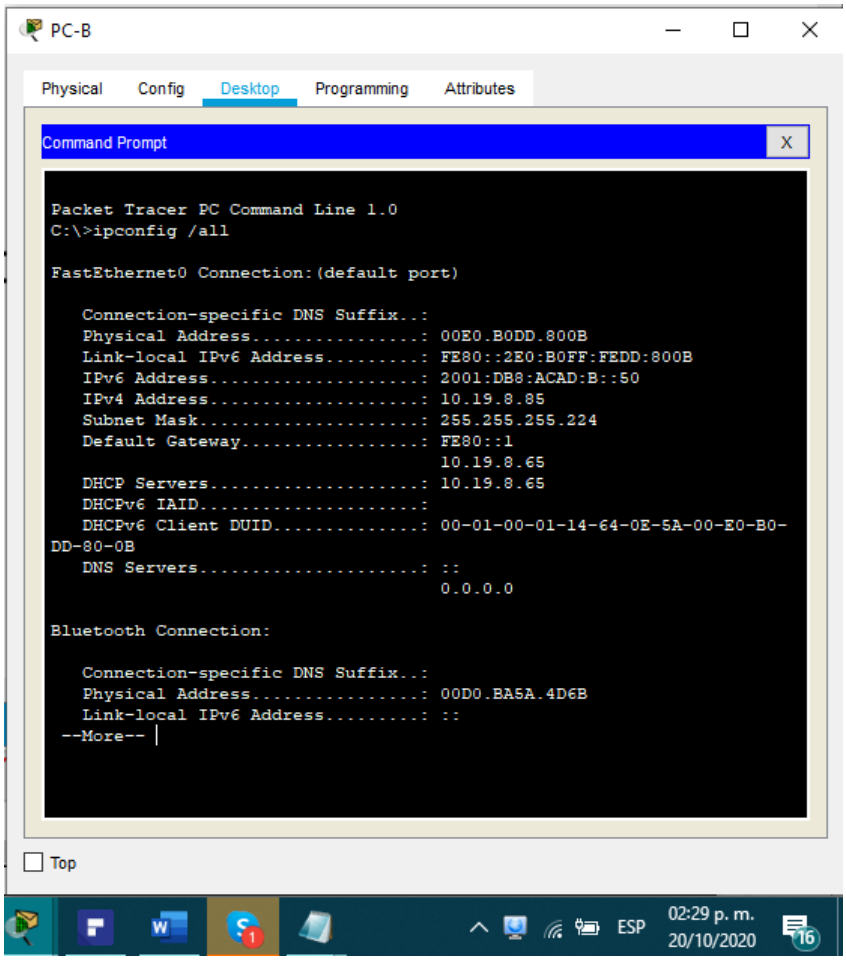
Fuente: Autor.

Se configura el direccionamiento IPv4 e IPv6 en PC-A, estableciendo la dirección, máscara de subred y el Gateway predeterminado.

Tabla 11. Configuración de red PC-B.

PC-B Network Configuration	
Descripción	Fastethernet0
Dirección física	00E0:B0DD:800B
Dirección IP	10.19.8.85 2001.DB8:ACAD:B::50
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 16. Configuración de red para PC-B.



Fuente: Autor.

Se configura el direccionamiento IPv4 e IPv6 en PC-B, estableciendo la dirección, máscara de subred y el Gateway predeterminado.

Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

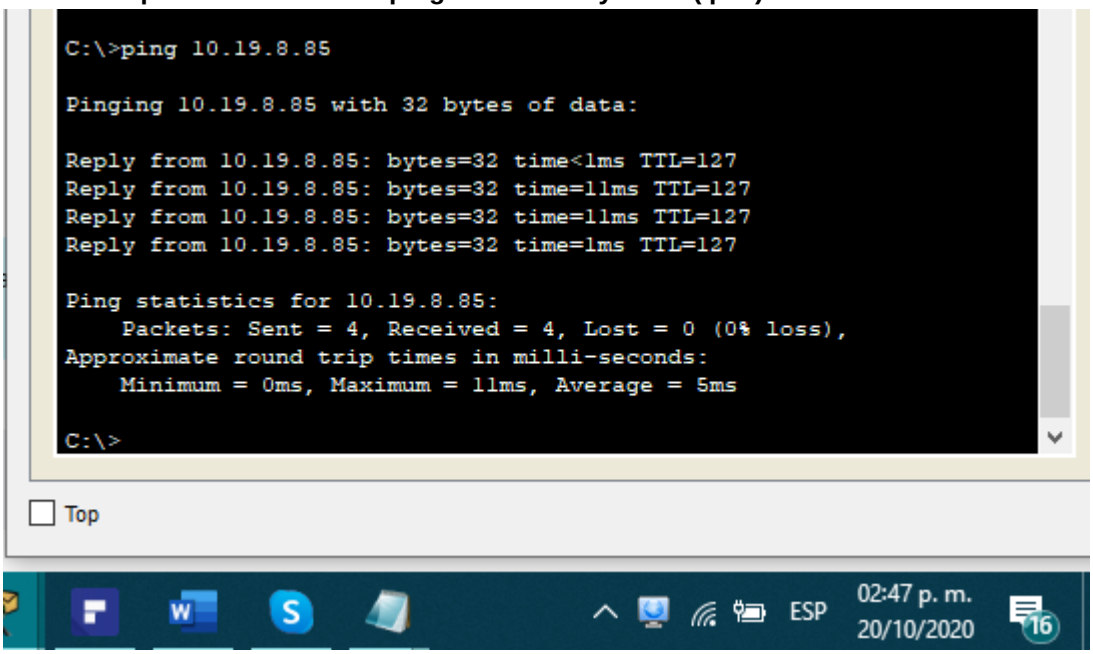
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Instrucciones para verificación de conectividad de extremo a extremo de la red.

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	**OK**
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	**OK**
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	**OK**
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	**OK**
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	**OK**
PC-A	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	**OK**
PC-A	S1, VLAN 4	Dirección	10.19.8.98	**OK**
PC-A	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	**OK**
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	**OK**
PC-A	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	**OK**
PC-A	PC-B	Dirección	10.19.8.85	**OK**
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	**OK**
PC-A	R1 Bucle 0	Dirección	209.165.201.1	**OK**
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	**OK**
PC-B	R1 Bucle 0	Dirección	209.165.201.1	**OK**
PC-B	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	**OK**
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	**OK**

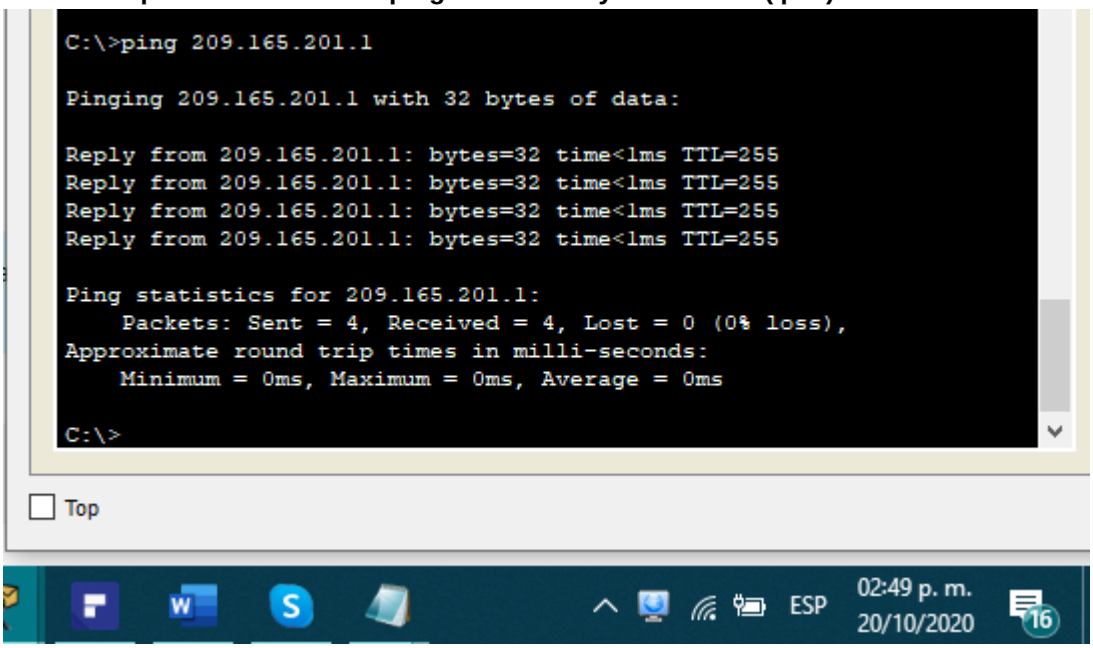
PC-B	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	**OK**
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	**OK**
PC-B	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	**OK**
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	**OK**
PC-B	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	**OK**
PC-B	S1, VLAN 4	Dirección	10.19.8.98	**OK**
PC-B	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	**OK**
PC-B	S2, VLAN 4	Dirección	10.19.8.99	**OK**
PC-B	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	**OK**

Figura 17. Respuesta al comando ping entre PC-A y PC-B (Ipv4).



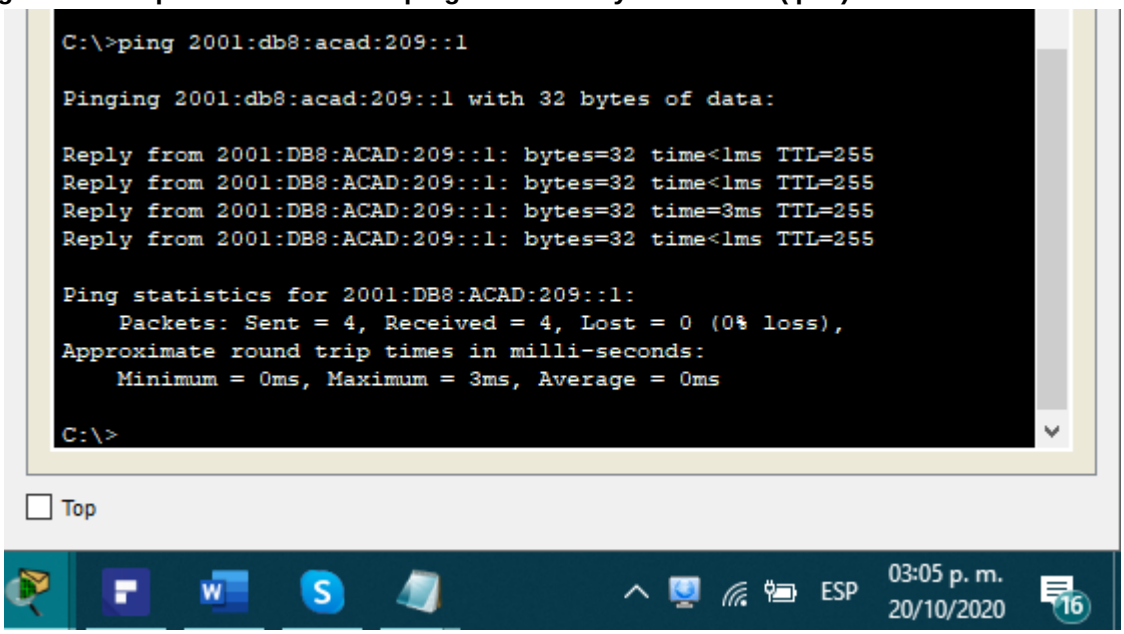
Fuente: Autor.

Figura 18. Respuesta al comando ping entre PC-A y R1 Bucle 0 (Ipv4).



Fuente: Autor.

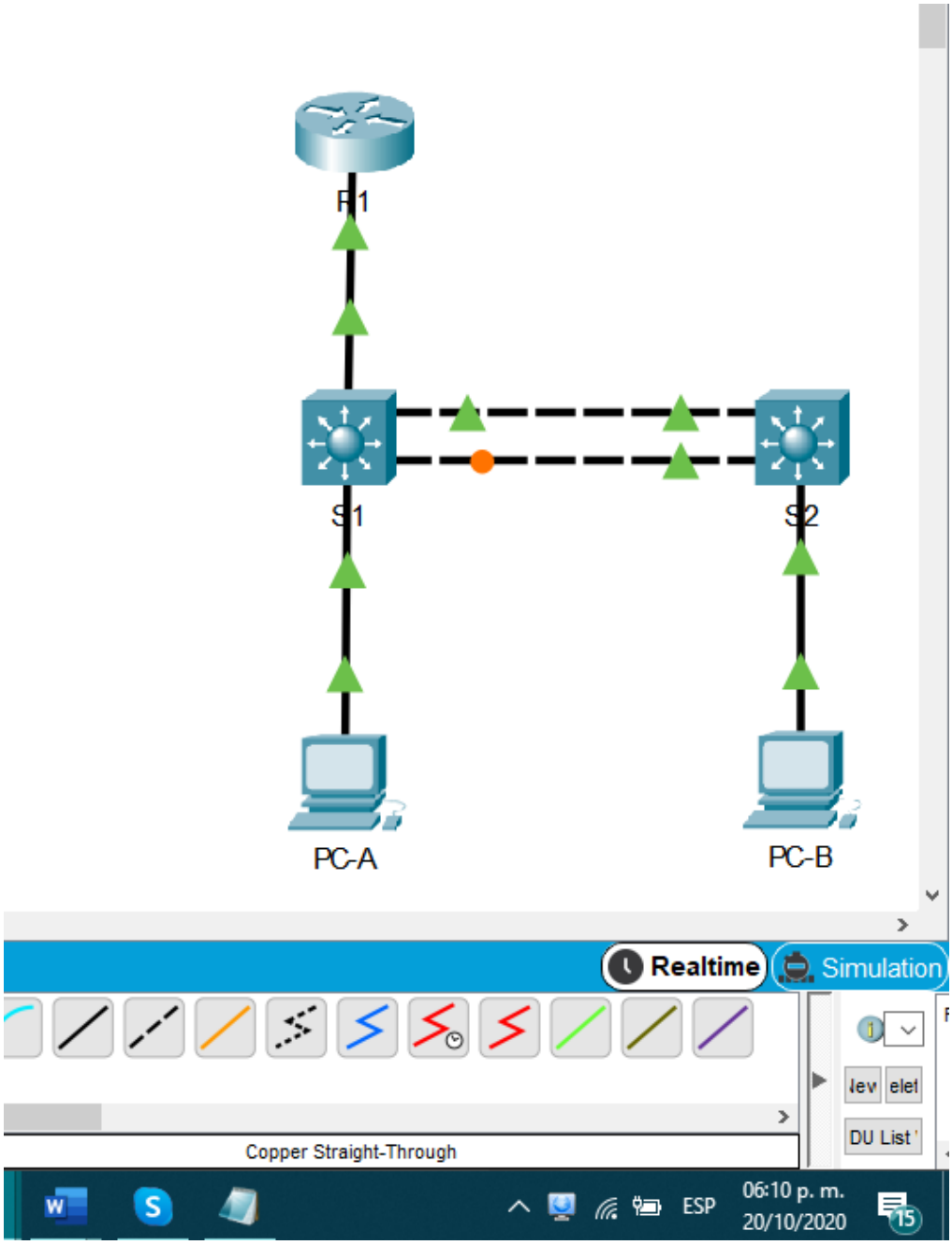
Figura 19. Respuesta al comando ping entre PC-B y R1 Bucle 0 (Ipv6).



Fuente: Autor.

Empleando el comando “ping” se valida la conectividad de los hosts (PC-A y PC-B) con las diferentes interfaces, subinterfaces y demás dispositivos de la red.

Figura 20. Topología final de la Red.

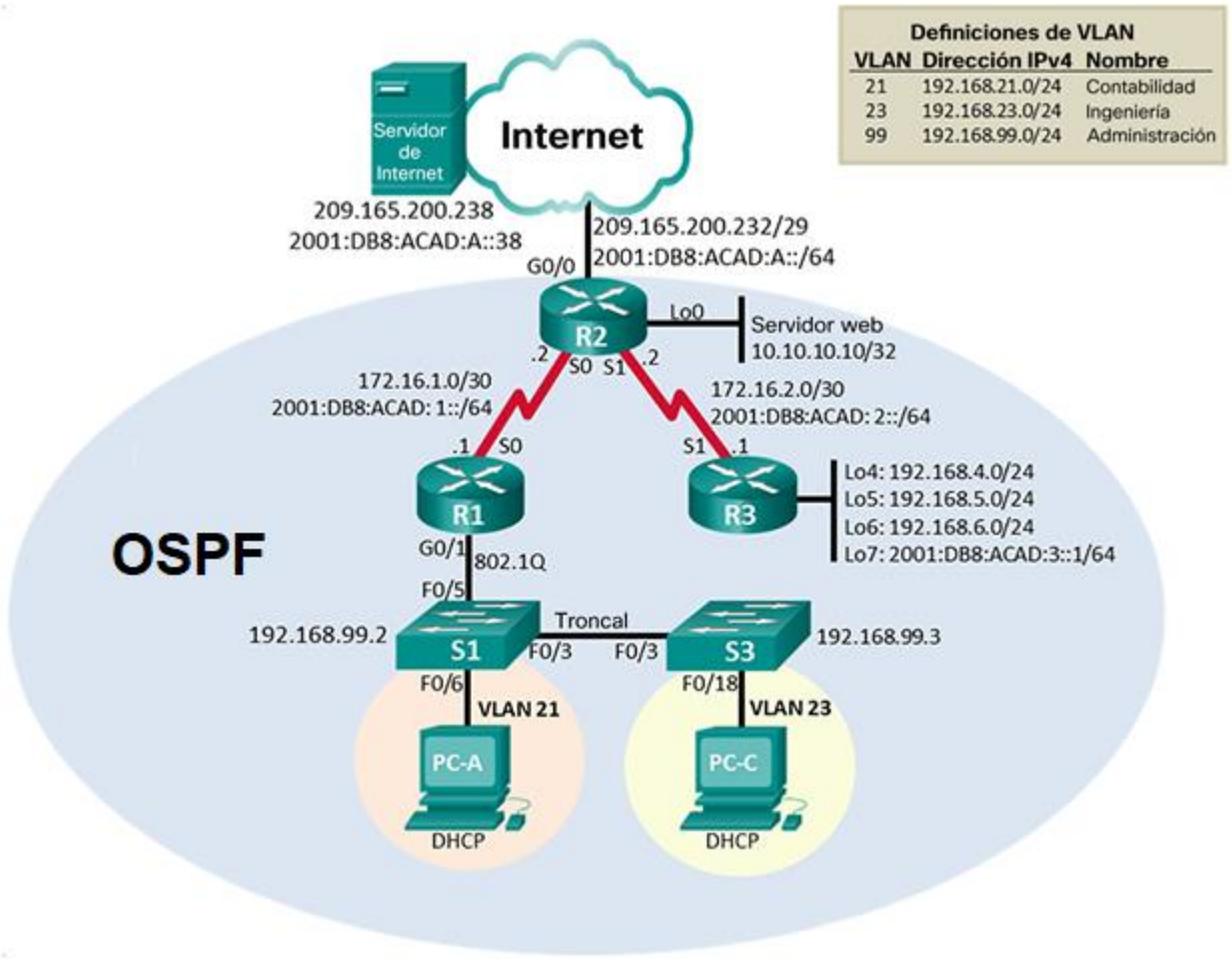


Fuente: Autor.

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 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 21. Topología Escenario 2.



Fuente: Repositorio UNAD.

Inicializar dispositivos

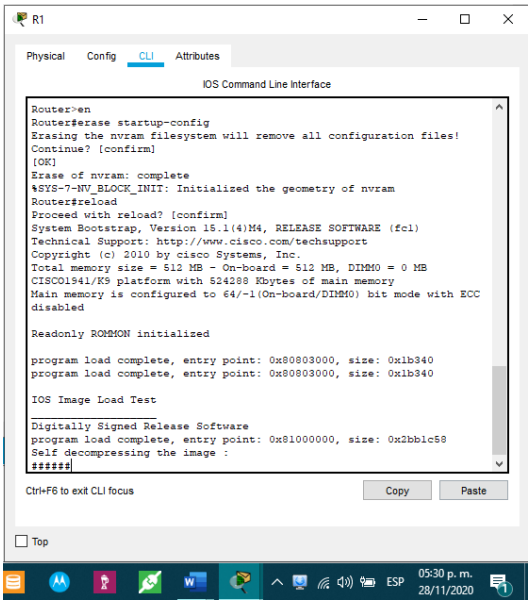
Inicializar y volver a cargar los routers y los switches.
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 13. Instrucciones y comandos de configuración para inicializar y volver a cargar los dispositivos de la red.

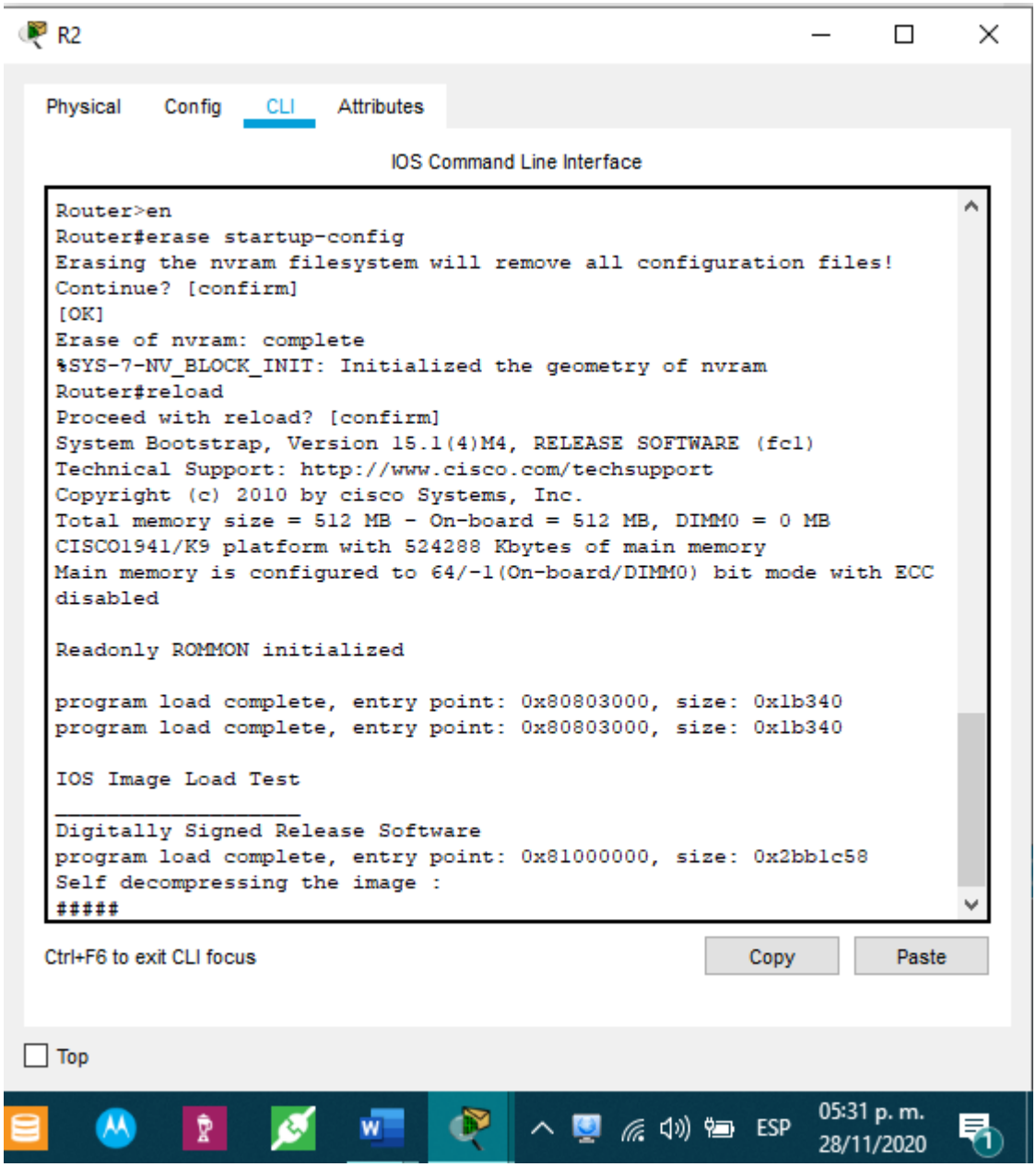
Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config delete vlan.dat
Volver a cargar ambos switches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

Figura 22. Eliminación de configuraciones de inicio y reinicio de R1.



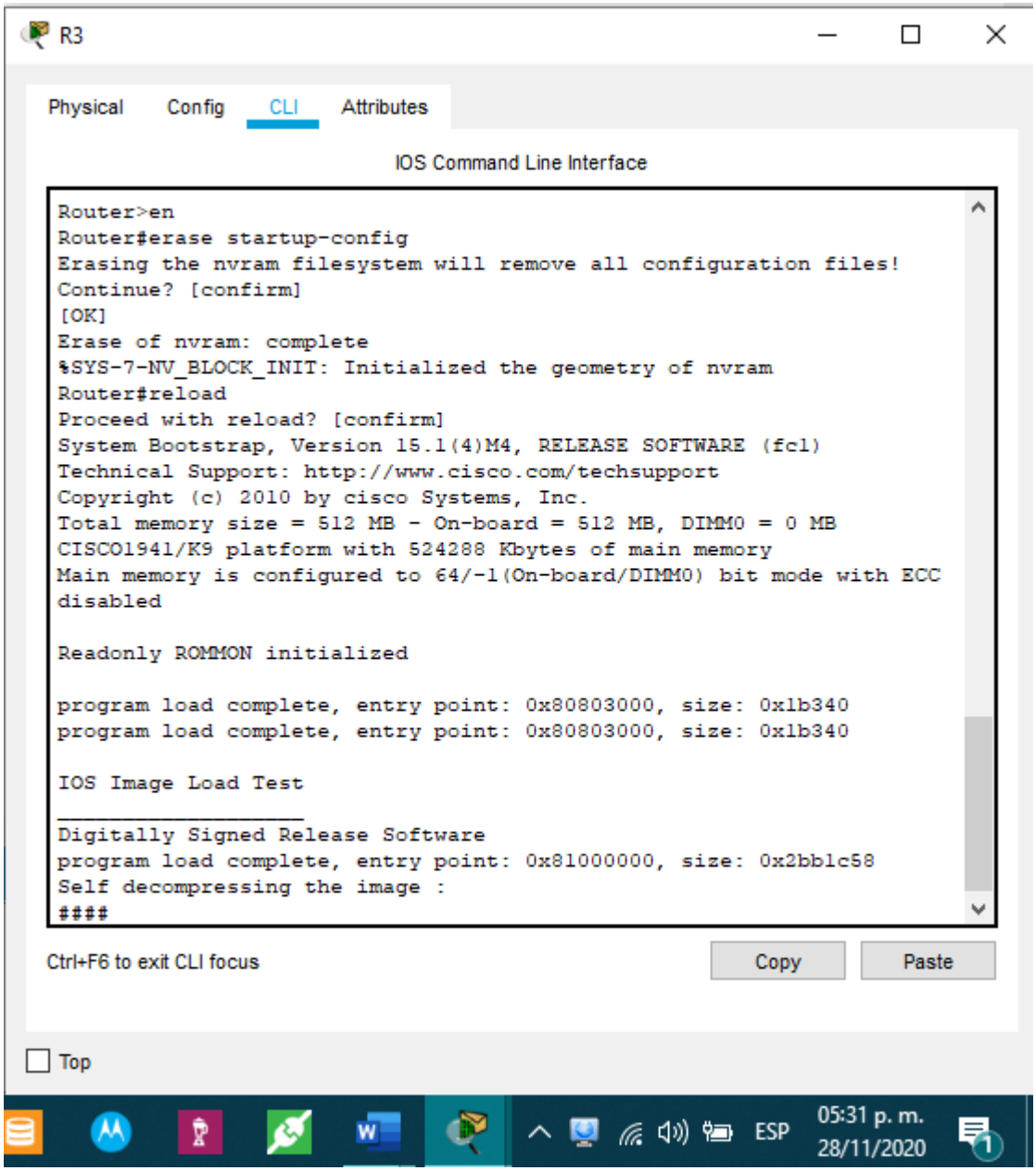
Fuente: Autor.

Figura 23. Eliminación de configuraciones de inicio y reinicio de R2.



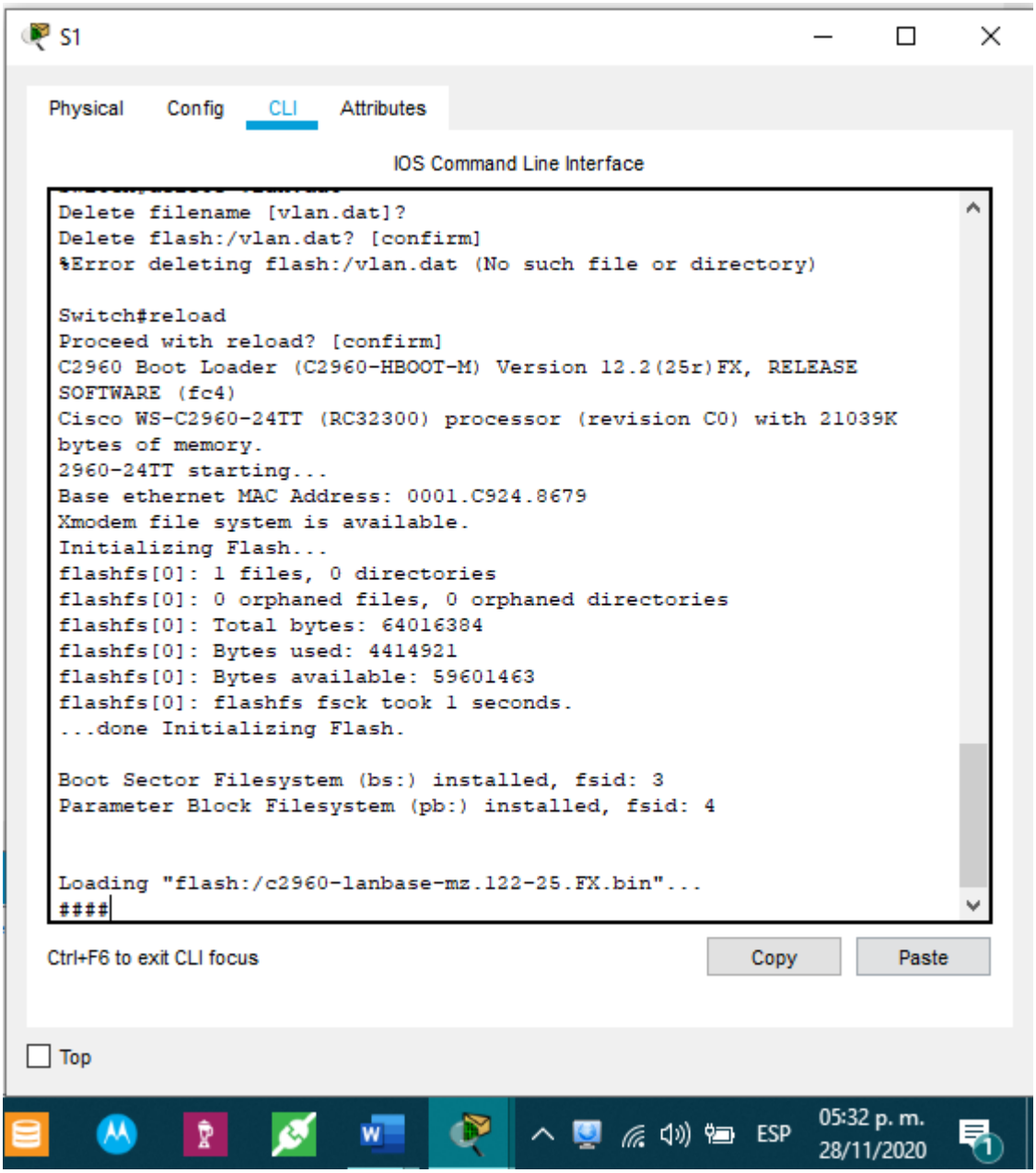
Fuente: Autor.

Figura 24. Eliminación de configuraciones de inicio y reinicio de R3.



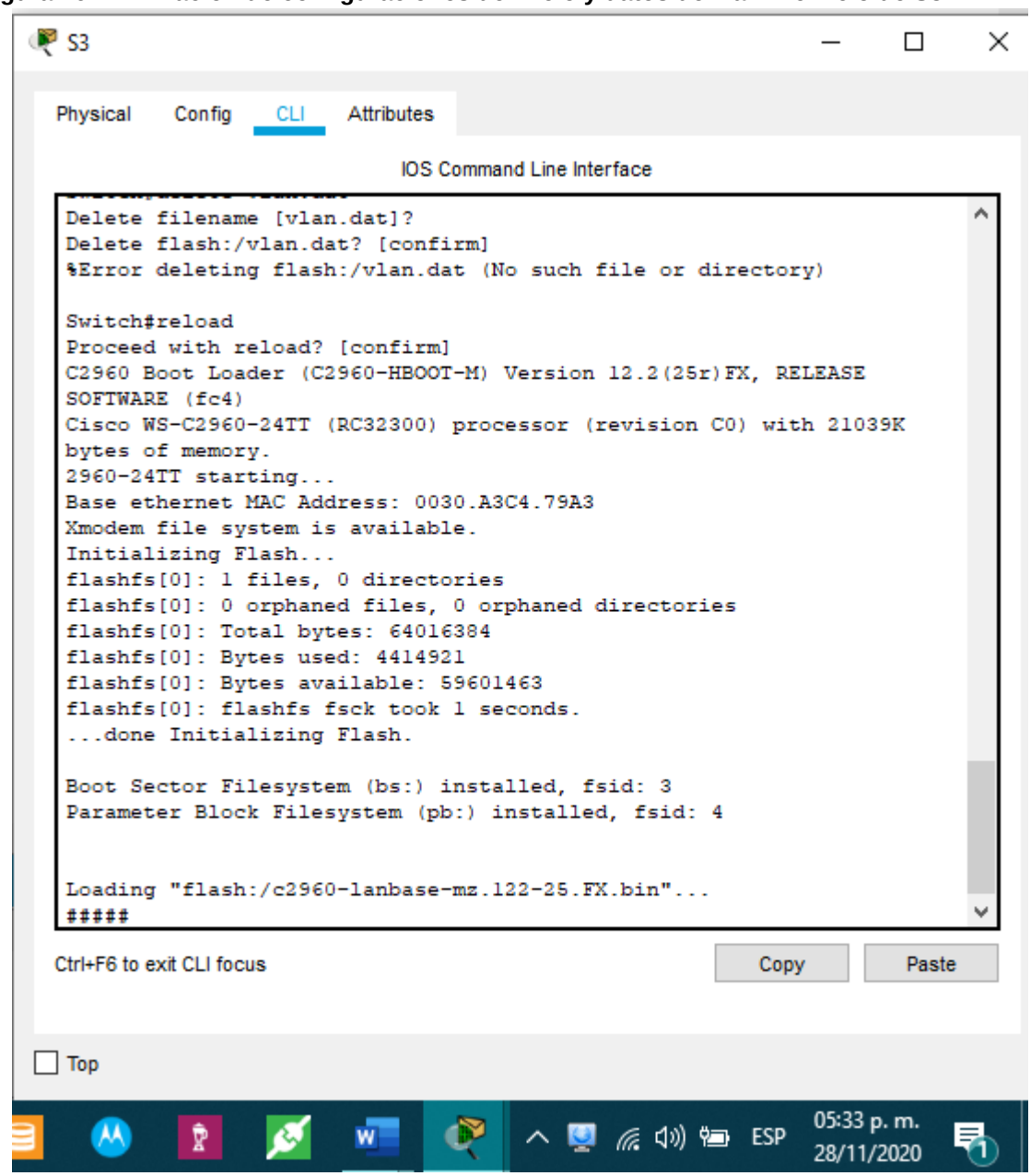
Fuente: Autor.

Figura 25. Eliminación de configuraciones de inicio y datos de vlan. Reinicio de S1.



Fuente: Autor.

Figura 26. Eliminación de configuraciones de inicio y datos de vlan. Reinicio de S3.



Fuente: Autor.

Como parte inicial se elimina cualquier tipo de configuración inicial presente en los routers y switches. Se borra la tabla de vlan de los conmutadores y se recargan todos los dispositivos para aplicar los cambios.

Configurar los parámetros básicos de los dispositivos

Configurar la computadora de Internet

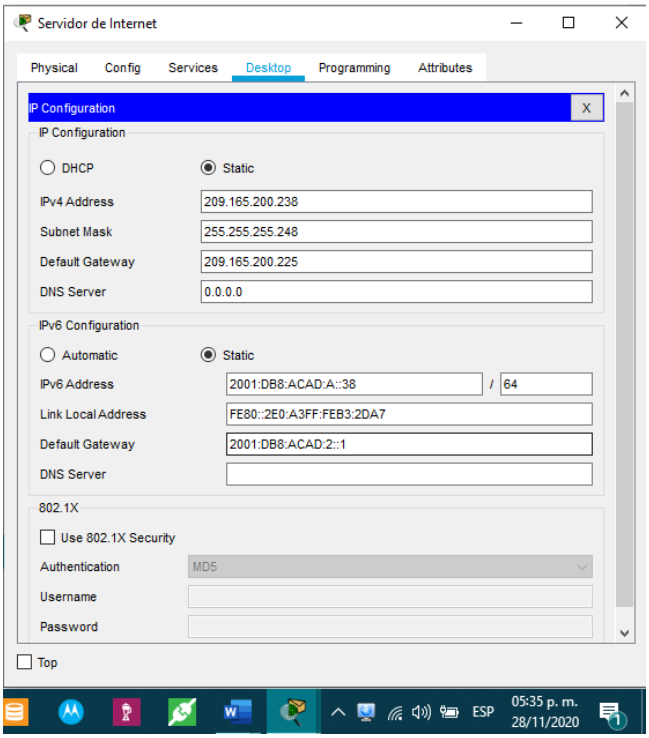
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 14. Instrucciones de configuración de red para Servidor de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

Figura 27. Configuración de red Servidor de Internet.



Fuente: Autor.

Establecemos el direccionamiento IPv4 e IPv6 estatico para el servidor de internet.

Configurar R1

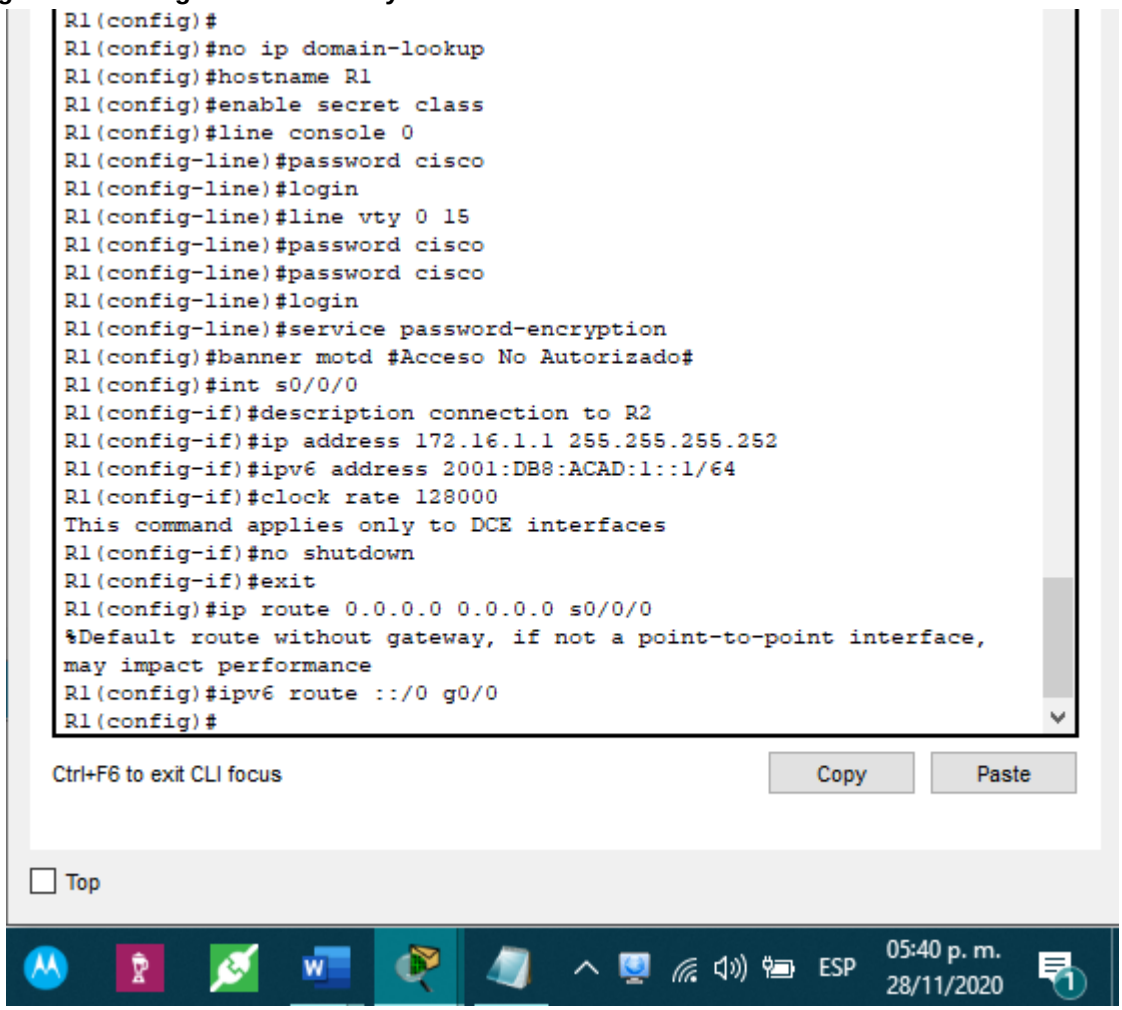
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Instrucciones y comandos para configuración básica y de interfaces en 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	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/0/0	description connection to R2 ip address 172.16.1.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::1/64 clock rate 128000 no shutdown exit
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 s0/0/0 ipv6 route ::/0 g0/0

Nota: Todavía no configure G0/1.

Figura 28. Configuración básica y de interfaces en R1.



Fuente: Autor.

Se establece la configuración inicial para R1. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados. Se asigna la descripción y direccionamiento IPv4 e IPv6 para la interfaz s0/0/0 y se crean las rutas estáticas.

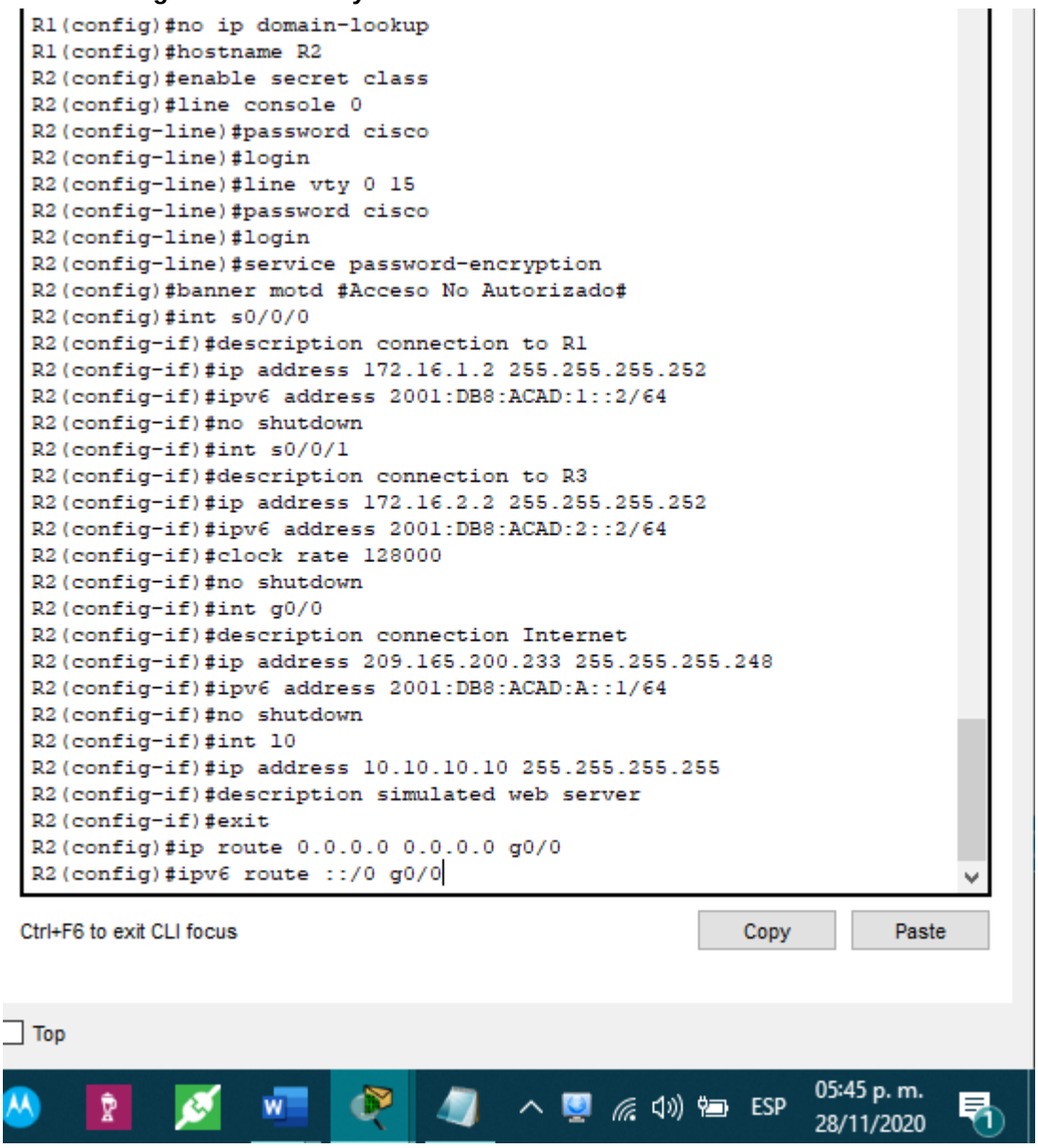
Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 16. Instrucciones y comandos para configuración básica y de interfaces en R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	hostname R2
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	Comando no soportado en el software Cisco Packet Tracer
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/0/0	int s0/0/0 description connection to R1 ip address 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::2/64 no shutdown
Interfaz S0/0/1	int s0/0/1 description connection to R3 ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::2/64 clock rate 128000 no shutdown
Interfaz G0/0 (simulación de Internet)	int g0/0 description connection Internet ip address 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64 no shutdown
Interfaz loopback 0 (servidor web simulado)	int l0 ip address 10.10.10.10 255.255.255.255 description simulated web server
Ruta predeterminada	ip route 0.0.0.0 0.0.0.0 g0/0 ipv6 route ::/0 g0/0

Figura 29. Configuración básica y de interfaces en R2.



Fuente: Autor.

Se establece la configuración inicial para R2. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados. Se asigna la descripción y direccionamiento IPv4 e IPv6 para las interfaces s0/0/0, s0/0/1, g0/0, Loppback0 y se crean las rutas estáticas.

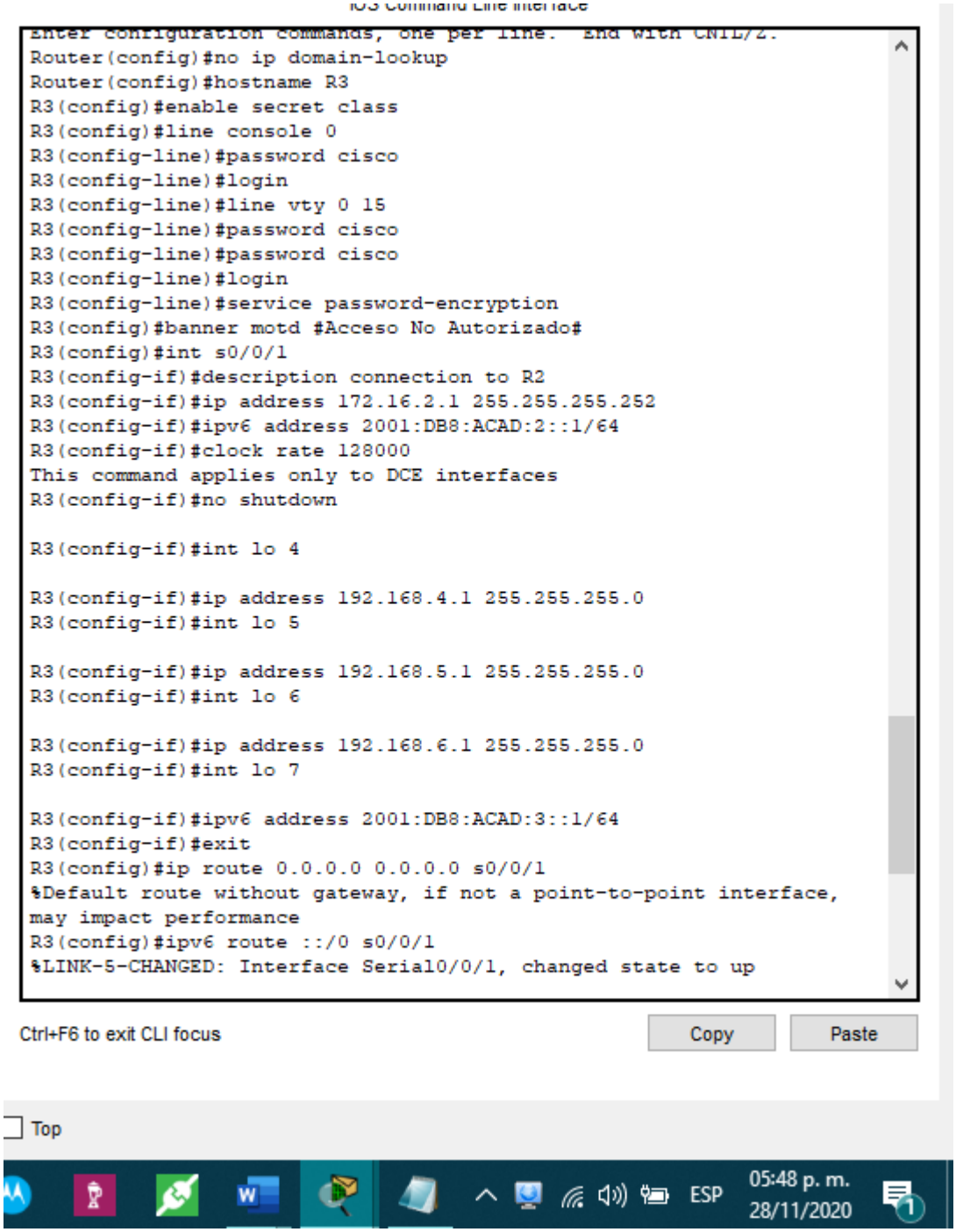
Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 17. Instrucciones y comandos para configuración básica y de interfaces en R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	hostname R3
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/0/1	int s0/0/1 description connection to R2 ip address 172.16.2.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::1/64 clock rate 128000 no shutdown
Interfaz loopback 4	int lo 4 ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	int lo 5 ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	int lo 6 ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	int lo 7 ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 s0/0/1 ipv6 route ::/0 s0/0/1

Figura 30. Configuración básica y de interfaces en R3.



Fuente: Autor.

Se establece la configuración inicial para R3. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso

y la creación de un banner de advertencia para los usuarios no autorizados. Se asigna la descripción y direccionamiento IPv4 e IPv6 para las interfaces s0/0/1, Loopback4, Loopback5, Loopback6, Loopback7 y se crean las rutas estáticas.

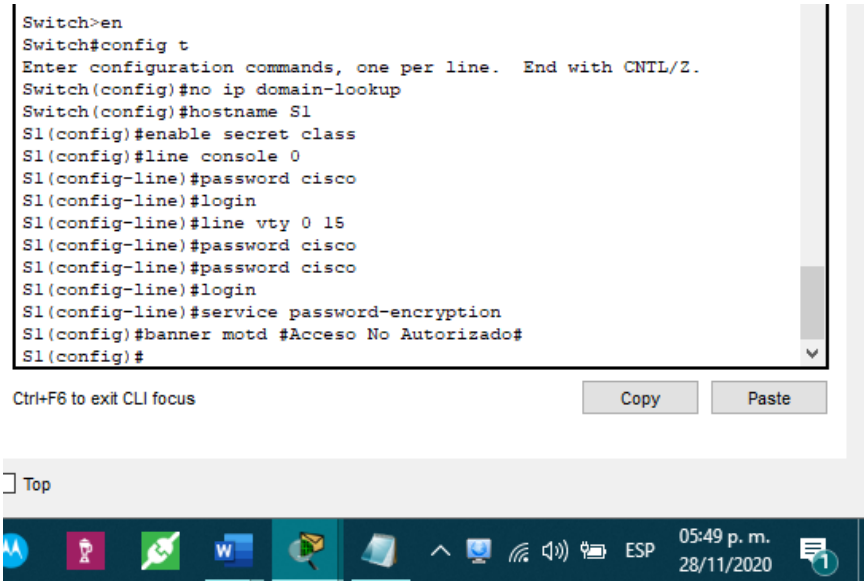
Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 18. Instrucciones y comandos para configuración básica en 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	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#

Figura 31. Configuración básica de S1.



Fuente: Autor.

Se establece la configuración inicial para S1. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados.

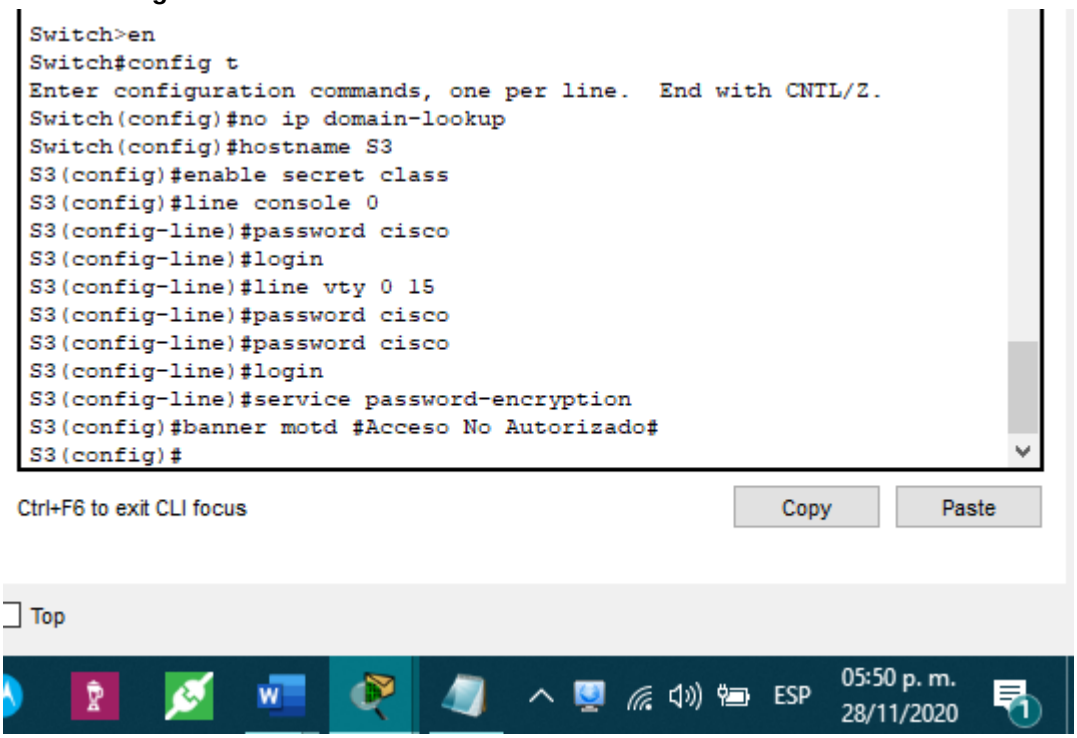
Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19. Instrucciones y comandos para configuración básica en S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	hostname S3
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#

Figura 32. Configuración básica de S3.



Fuente: Autor.

Se establece la configuración inicial para S3. Como aspectos más importantes tenemos la asignación de un nombre, dominio, la seguridad de las líneas de acceso y la creación de un banner de advertencia para los usuarios no autorizados.

Verificar la conectividad de la red

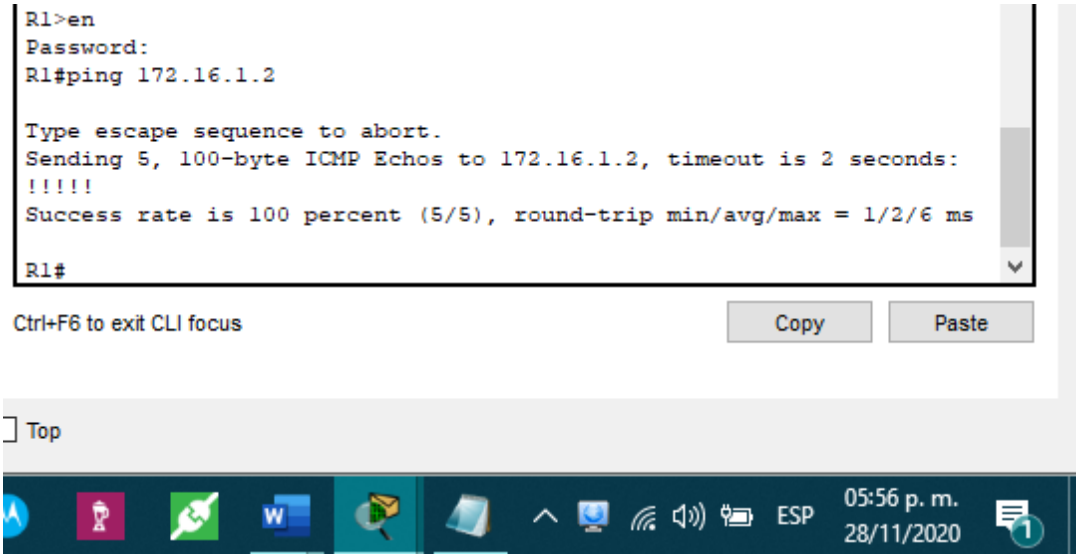
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20. Instrucciones para verificación de conectividad de la red.

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

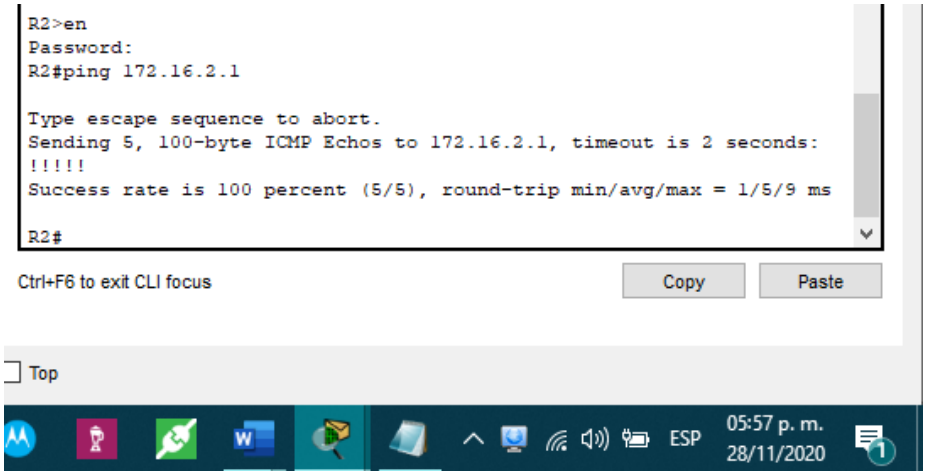
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 33. Ping desde R1 a interfaz S0/0/0 de R2.



Fuente: Autor.

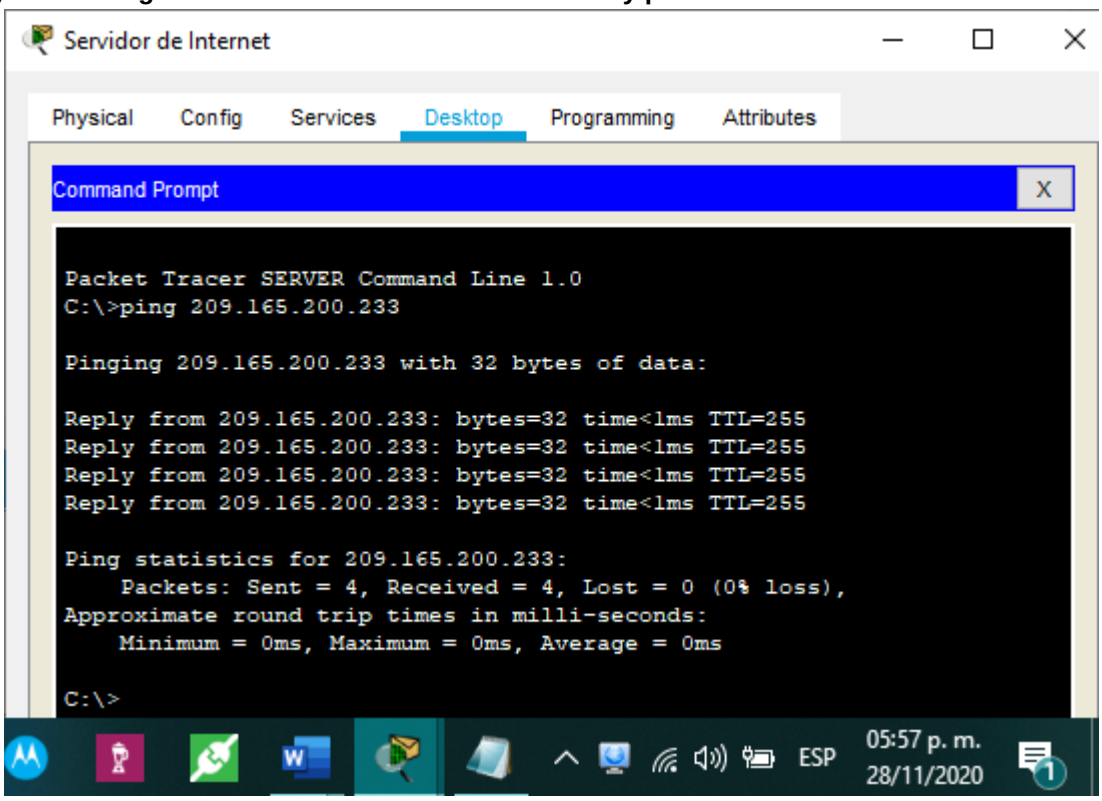
Figura 34. Ping desde R2 a interfaz S0/0/1 de R3.



Fuente: Autor.

Empleando el comando “ping” verificamos la conectividad entre los enrutadores de nuestra red.

Figura 35. Ping desde Servidor de Internet a Gateway predeterminado.



Fuente: Autor.

Empleando el comando “ping” verificamos la conectividad entre el Servidor de Internet y el Gateway predeterminado.

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

Configurar S1

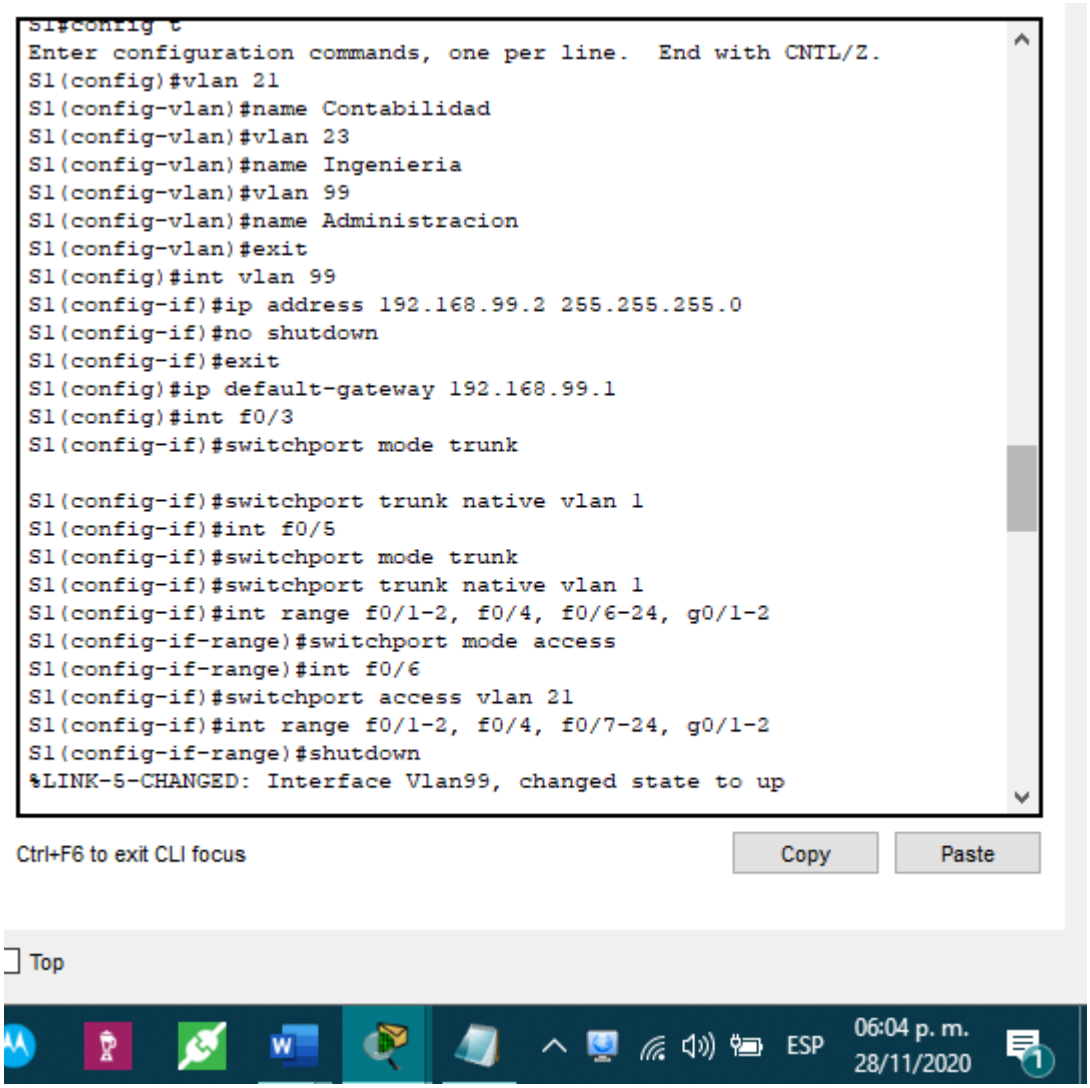
La configuración del S1 incluye las siguientes tareas:

Tabla 21. Instrucciones y comandos de configuración de seguridad, vlan y routing entre vlan en S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion

Asignar la dirección IP de administración.	int vlan 99 ip address 192.168.99.2 255.255.255.0 no shutdown
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	int f0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4, f0/6-24, g0/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	int f0/6 switchport access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4, f0/7-24, g0/1-2 shut

Figura 36. Configuración de seguridad. Vlan y routing entre Vlan en S1.



Fuente: Autor.

Se crean las VLAN en S1 con su respectivo nombre y direccionamiento IP. Se establecen los enlaces troncales y los puertos de acceso para las diferentes Vlan. Se configura la seguridad y protección de las demás interfaces. Se deshabilitan las interfaces que no están en uso.

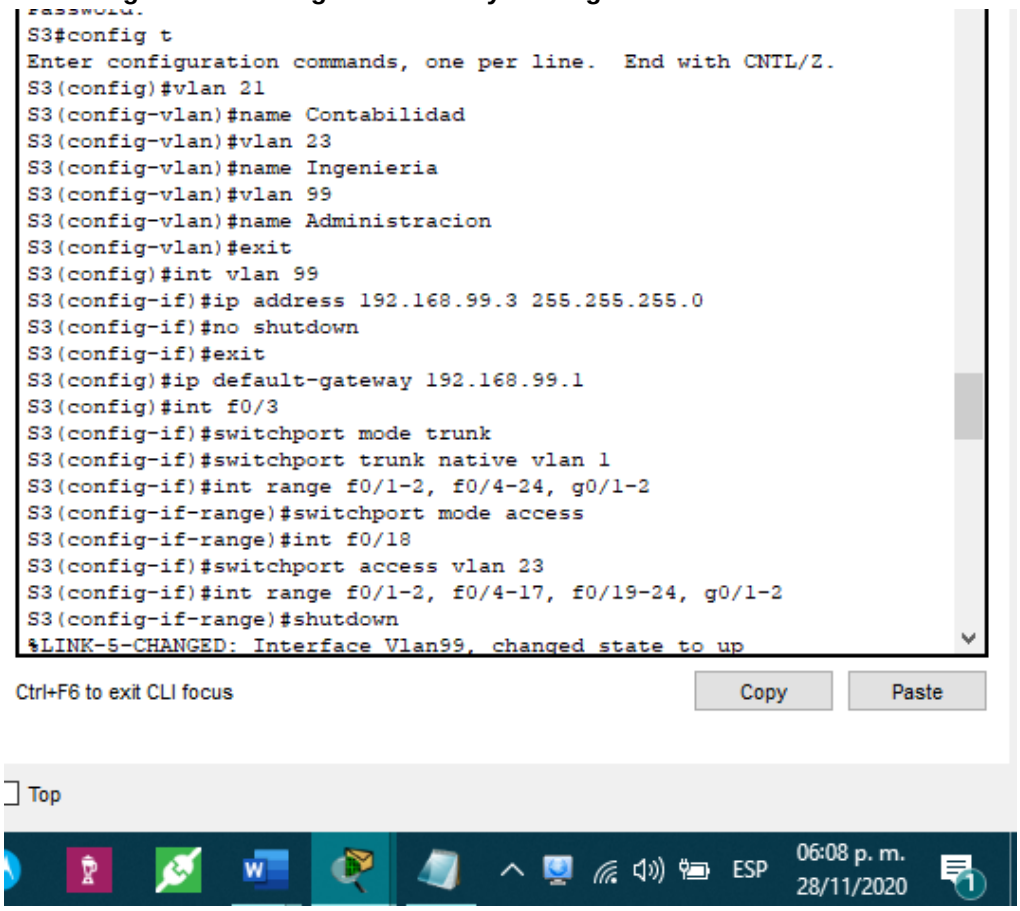
Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 22. Instrucciones y comandos de configuración de seguridad, vlan y routing entre vlan en S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion
Asignar la dirección IP de administración	int vlan 99 ip address 192.168.99.3 255.255.255.0 no shutdown
Asignar el gateway predeterminado.	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4-24, g0/1-2 switchport mode access
Asignar F0/18 a la VLAN 21	int f0/18 switchport access vlan 23
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Figura 37. Configuración de seguridad. Vlan y routing entre Vlan en S3.



Fuente: Autor.

Se crean las VLAN en S3 con su respectivo nombre y direccionamiento IP. Se establecen los enlaces troncales y los puertos de acceso para las diferentes Vlan. Se configura la seguridad y protección de las demás interfaces. Se deshabilitan las interfaces que no están en uso.

Configurar R1

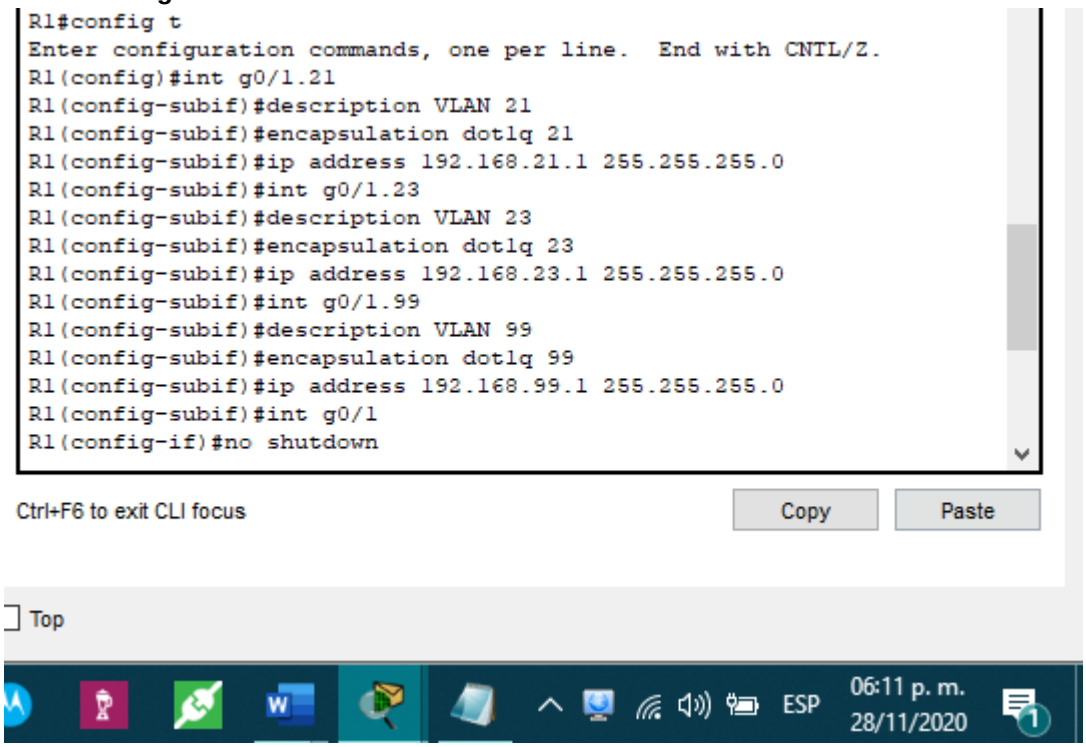
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Instrucciones y comandos de configuración de subinterfacez en R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	int g0/1.21 description VLAN 21 encapsulation dot1q 21

	ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	int g0/1.23 description VLAN 23 encapsulation dot1q 23 ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	int g0/1.99 description VLAN 99 encapsulation dot1q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	int g0/1 no shutdown

Figura 38. Configuración de subinterfaces en R1.



Fuente: Autor.

Se configuran las subinterfaces en R1 para cada VLAN estableciendo una descripción y su respectivo direccionamiento IP. Encendemos la interfaz con el comando “no shut”.

Verificar la conectividad de la red

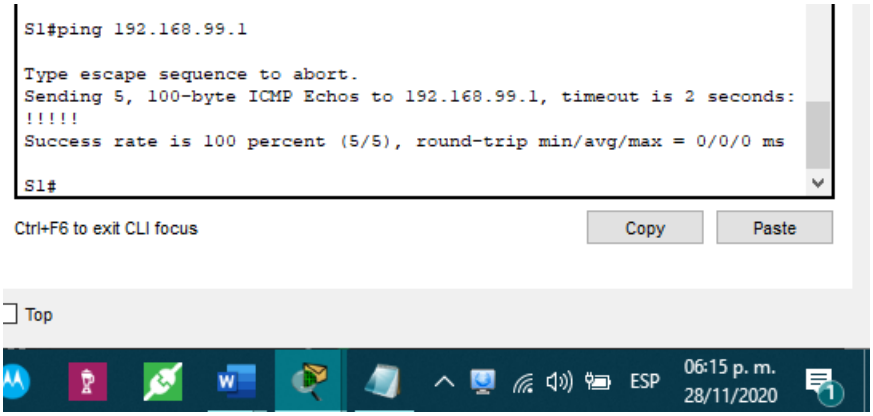
Utilice el comando ping para probar la conectividad entre los switches y el R1.

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 24. Instrucciones para verificar la conectividad de la red.

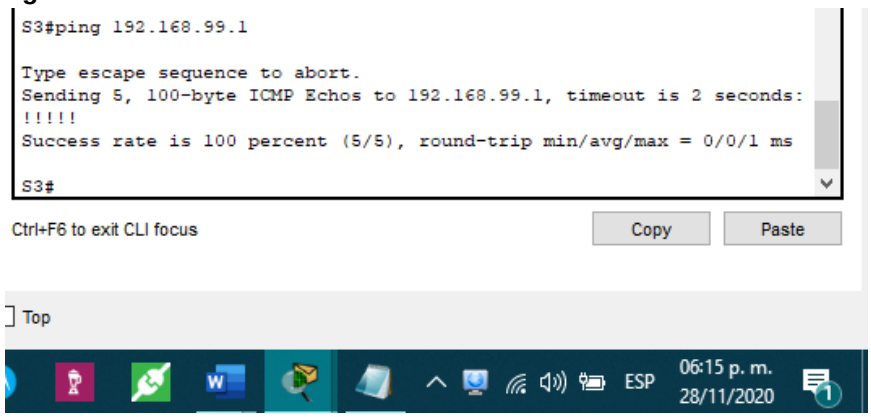
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	**Exitoso**
S3	R1, dirección VLAN 99	192.168.99.1	**Exitoso**
S1	R1, dirección VLAN 21	192.168.21.1	**Exitoso**
S3	R1, dirección VLAN 23	192.168.23.1	**Exitoso**

Figura 39. Ping desde S1 hacia dirección IP vlan 99 en R1.



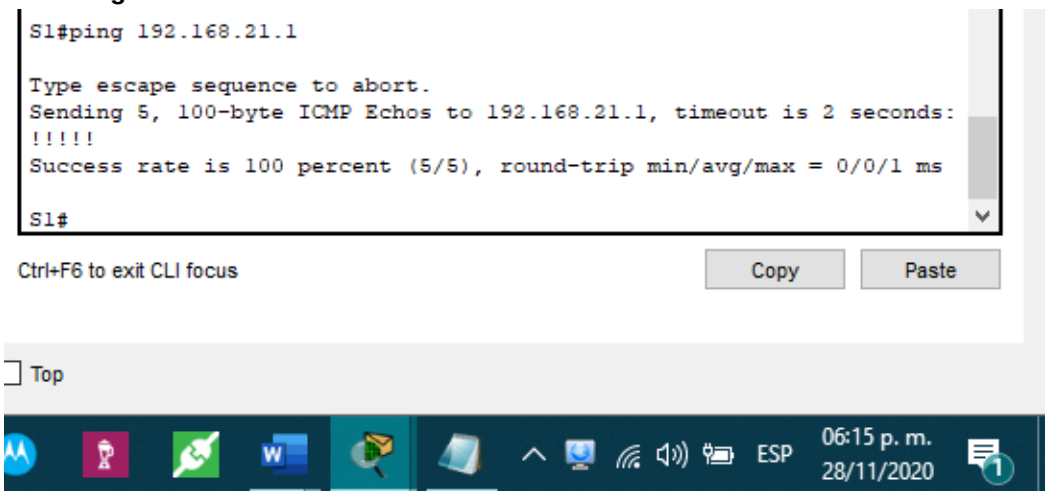
Fuente: Autor.

Figura 40. Ping desde S3 hacia dirección IP vlan 99 en R1.



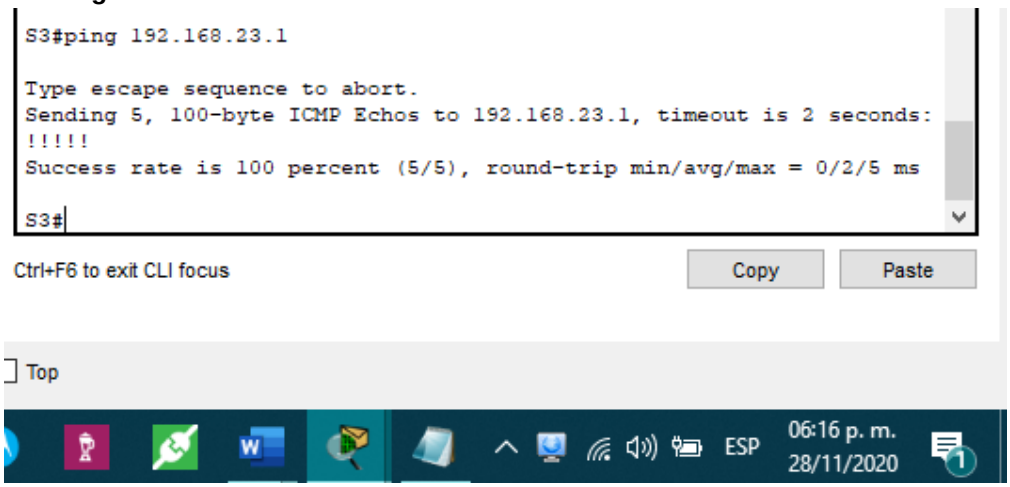
Fuente: Autor.

Figura 41. Ping desde S1 hacia dirección IP vlan 21 en R1.



Fuente: Autor.

Figura 42. Ping desde S3 hacia dirección IP vlan 23 en R1.



Fuente: Autor.

Verificación de conectividad desde los conmutadores a las subinterfaces asignadas a las Vlan en el enrutador empleando el comando “ping”.

Configurar el protocolo de routing dinámico OSPF

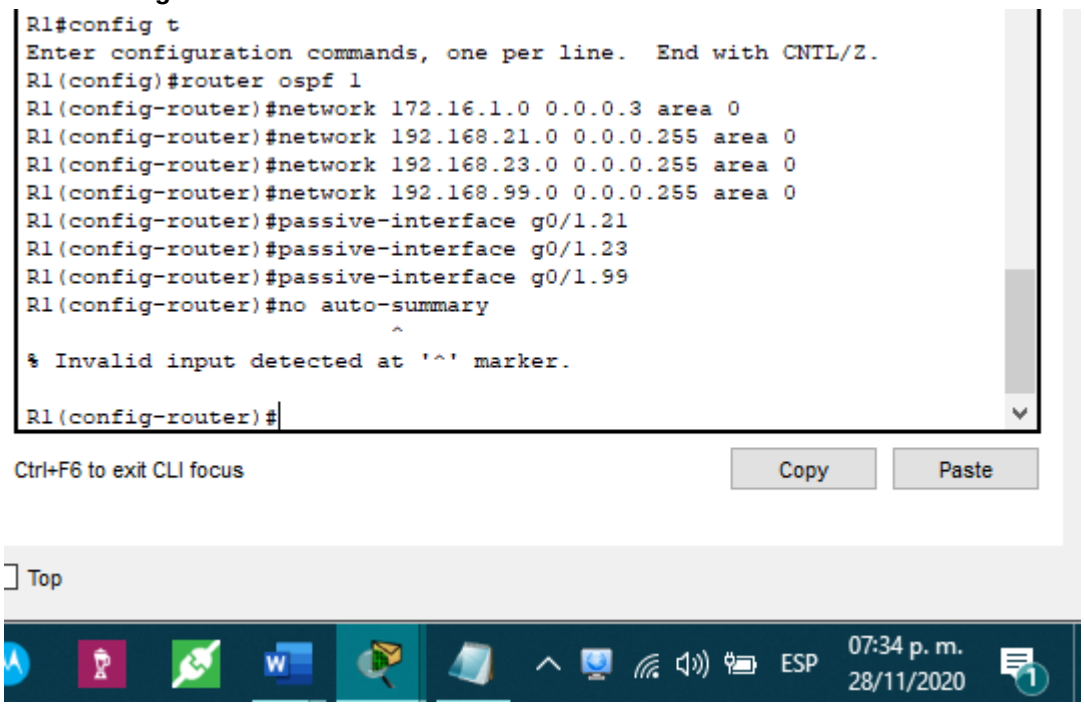
Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 25. Instrucciones y comandos de configuración protocolo OSPF en R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	OSPF no tiene sumarización automática

Figura 43. Configuración OSPF en R1.



Fuente: Autor.

Se crea el enrutamiento dinamico OSPFv2 en R1 determinando las rutas y estableciendo las interfaces como pasivas. Este protocolo no tiene sumarización automática.

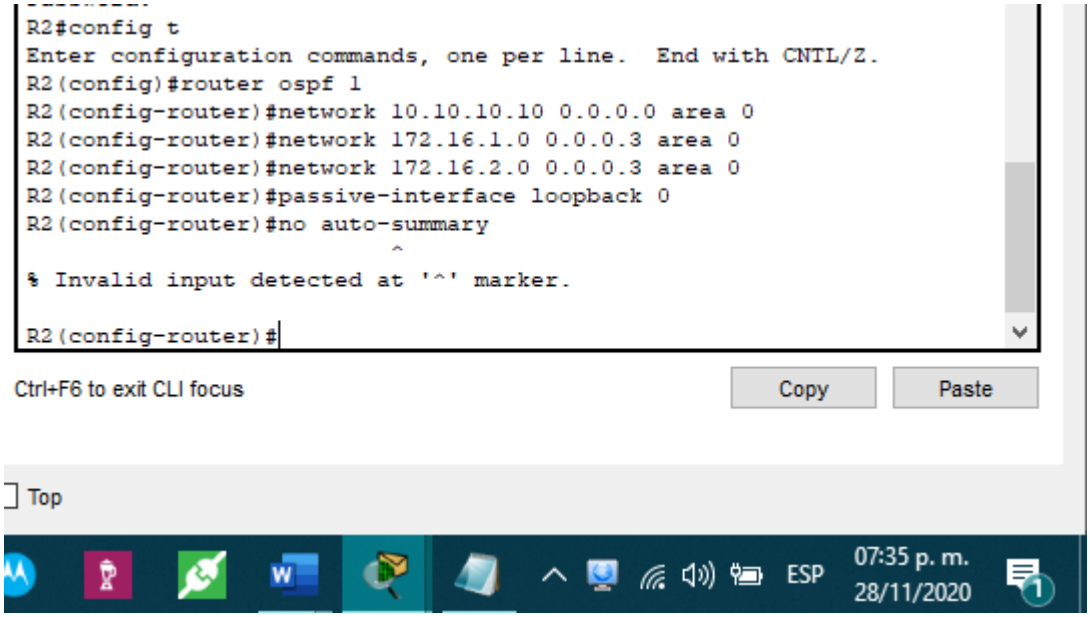
Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 26. Instrucciones y comandos de configuración de protocolo OSPF en R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	network 10.10.10.10 0.0.0.0 area 0 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	OSPF no tiene sumarización automática

Figura 44. Configuración OSPF en R2.



Fuente: Autor.

Se crea el enrutamiento dinamico OSPFv2 en R2 determinando las rutas y estableciendo las interfaces como pasivas. Este protocolo no tiene sumarización automática.

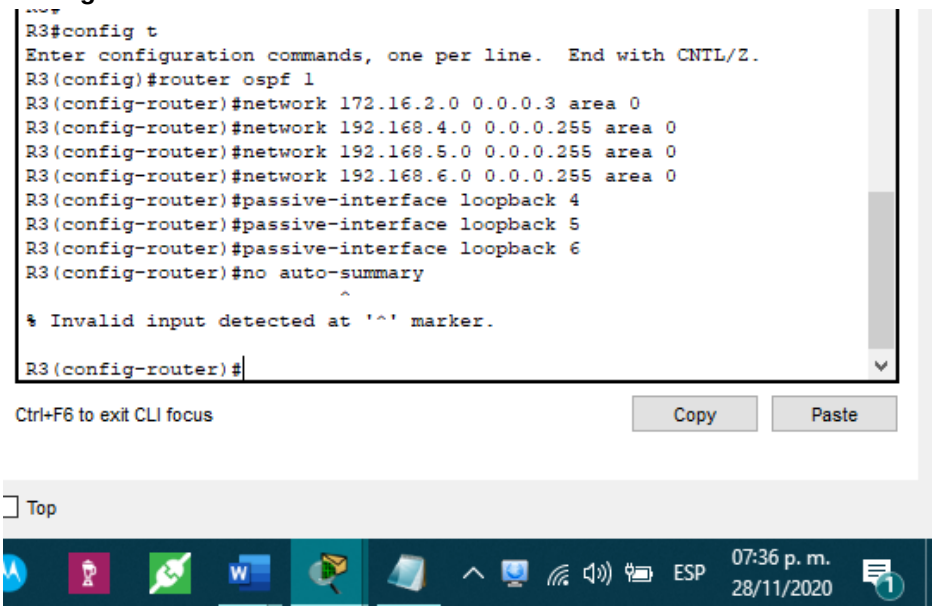
Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 27. Instrucciones y comandos de configuración de protocolos OSPF y OSPFv3 en R3.

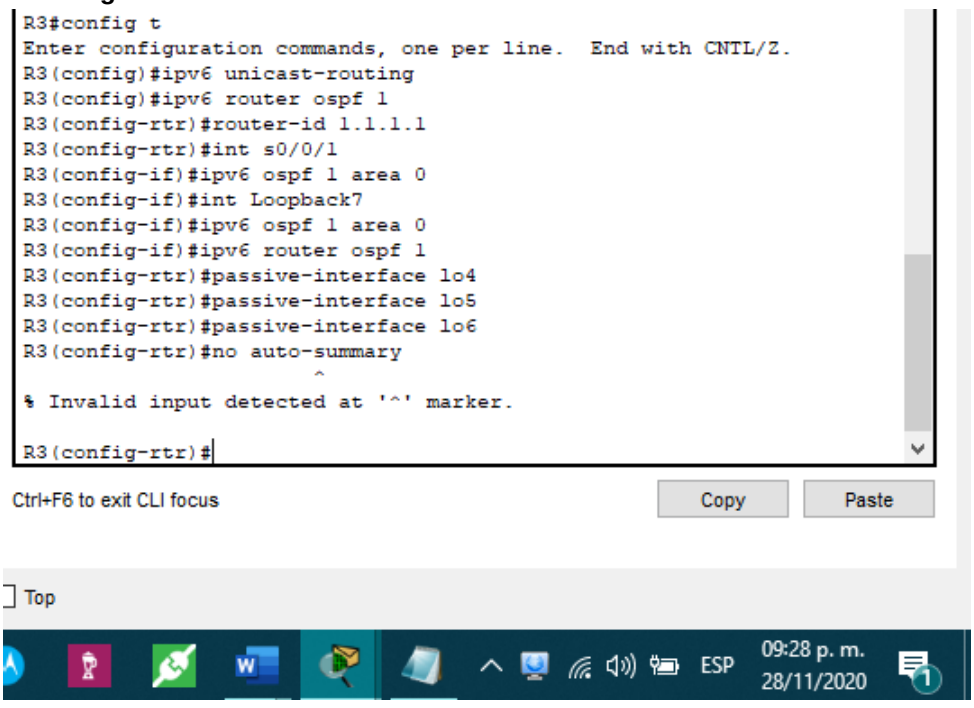
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	IPv4: router ospf 1 IPv6: ipv6 unicast-routing ipv6 router ospf 1 router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	IPv4: network 172.16.2.0 0.0.0.3 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0 IPv6: int s0/0/1 ipv6 ospf 1 area 0 int Loopback7 ipv6 ospf 1 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	IPv4: passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6 IPv6: passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	OSPF no tiene sumarización automática

Figura 45. Configuración OSPF en R3.



Fuente: Autor.

Figura 46. Configuración OSPFv3 en R3.



Fuente: Autor.

Se crea el enrutamiento dinamico OSPFv2 y OSPFv3 en R3 determinando las rutas y estableciendo las interfaces como pasivas. Este protocolo no tiene sumarización automática.

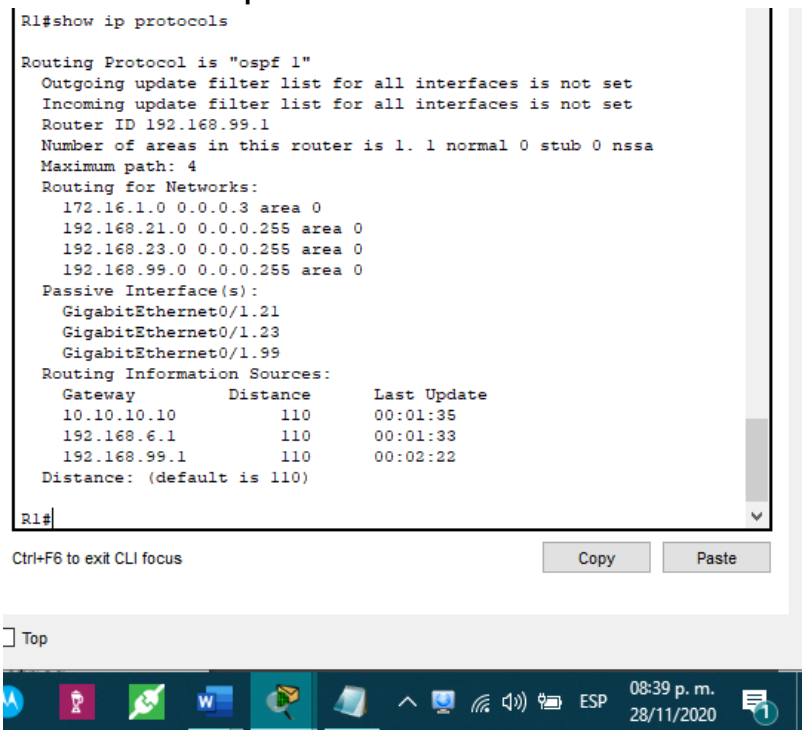
Verificar la información de OSPF

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

Tabla 28. Verificación protocolo OSPF.

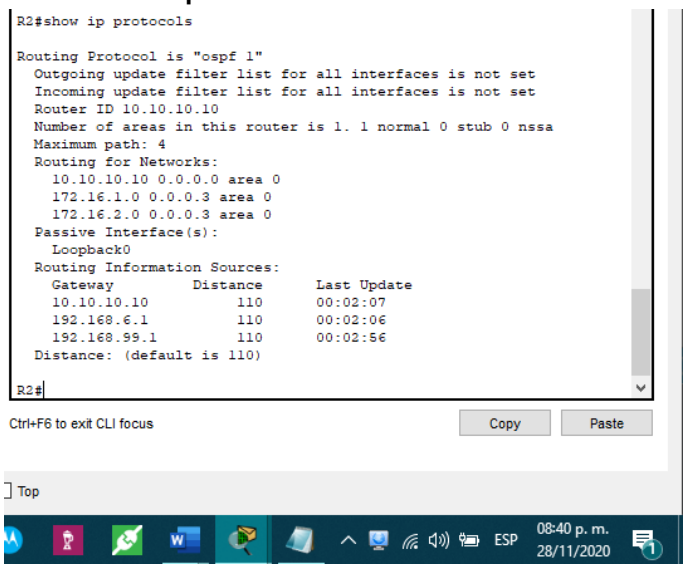
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración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

Figura 47. Verificación estado del protocolo OSPF en R1.



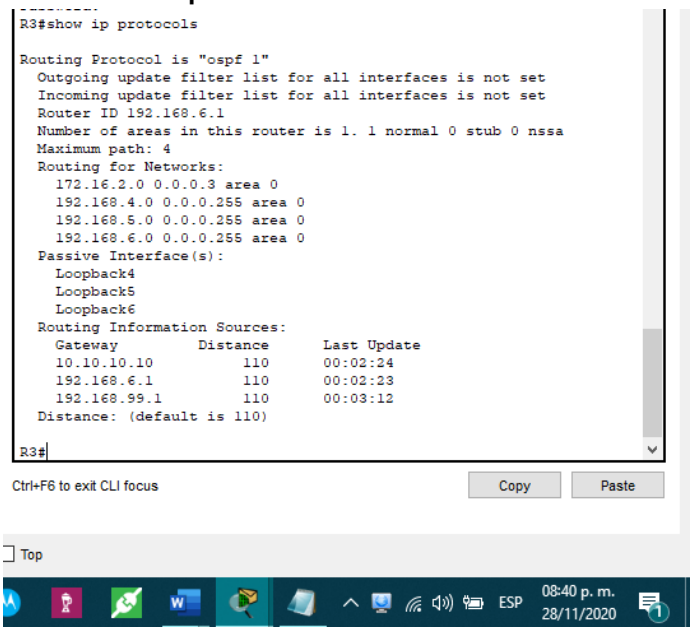
Fuente: Autor.

Figura 48. Verificación estado del protocolo OSPF en R2.



Fuente: Autor.

Figura 49. Verificación estado del protocolo OSPF en R3.



Fuente: Autor.

Empleando el comando “show ip protocols” verificamos que se haya configurado correctamente los protocolos OSPFv2 y OSPFv3 en los enrutadores R1, R2 y R3 de la red.

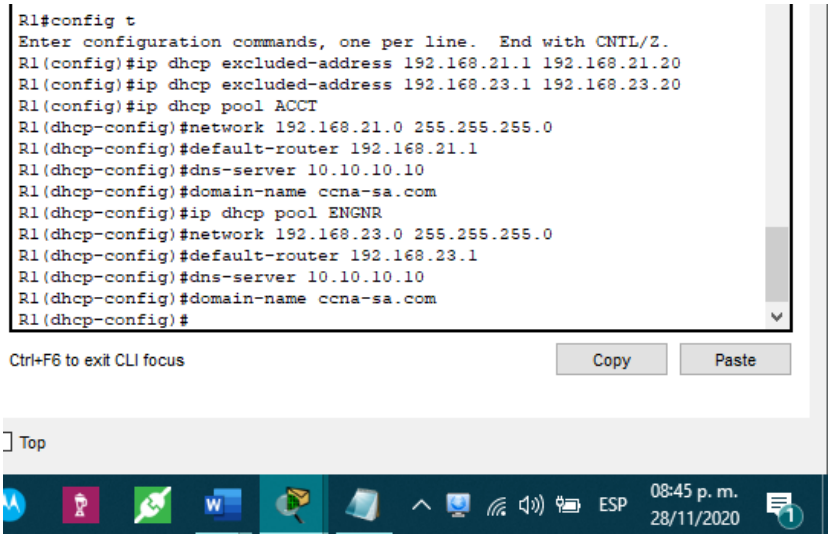
Implementar DHCP y NAT para IPv4

Configurar el R1 como servidor de DHCP para las VLAN 21 y 23
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 29. Instrucciones y comandos de configuración DHCP en R1.

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

Figura 50. Configuración servidor DHCP en R1.



Fuente: Autor.

Configuramos el servidor DHCP para R1 creando el pool, asignando la red, el dominio y el default-router. También se realiza la reserva de las primeras 20 direcciones IP en cada subred.

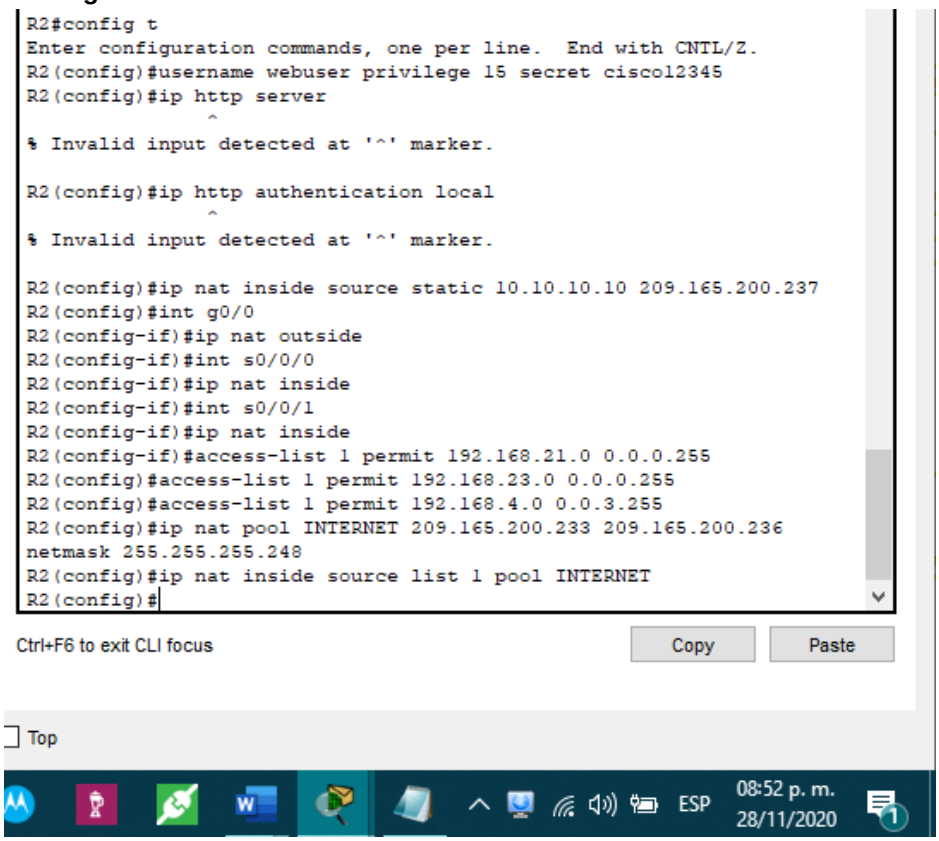
Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 30. Instrucciones y comandos de configuración NAT en R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Ip http server Comando no soportado en Cisco Packet Tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Ip http authentication local Comando no soportado en Cisco Packet Tracer
Crear una NAT estática al servidor web.	ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	int g0/0 ip nat outside int s0/0/0 ip nat inside int s0/0/1 ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Figura 51. Configuración NAT en R2.



Fuente: Autor.

Creamos la NAT estatica y le asignamos la interfaz interna y externa. Configuramos la NAT dinamica creando las listas de acceso para las redes, definiendo el pool de direcciones públicas y la lista de traducción NAT dinámica.

Verificar el protocolo DHCP y la NAT estática

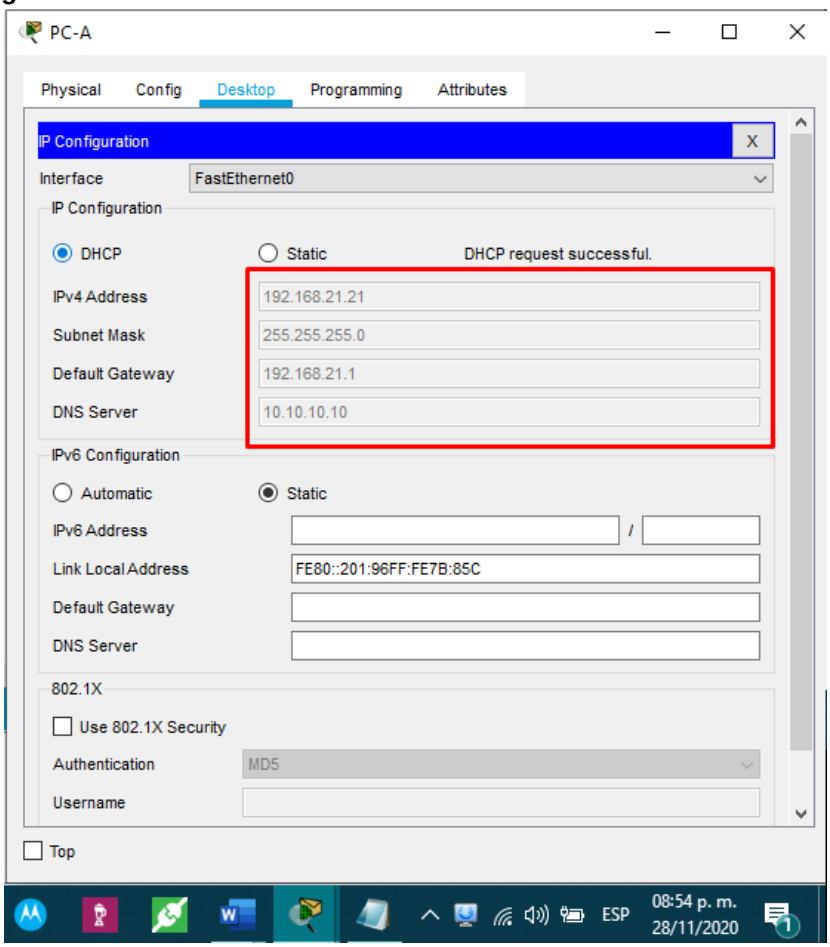
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 31. Verificación de protocolo DHCP y servicio NAT.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso

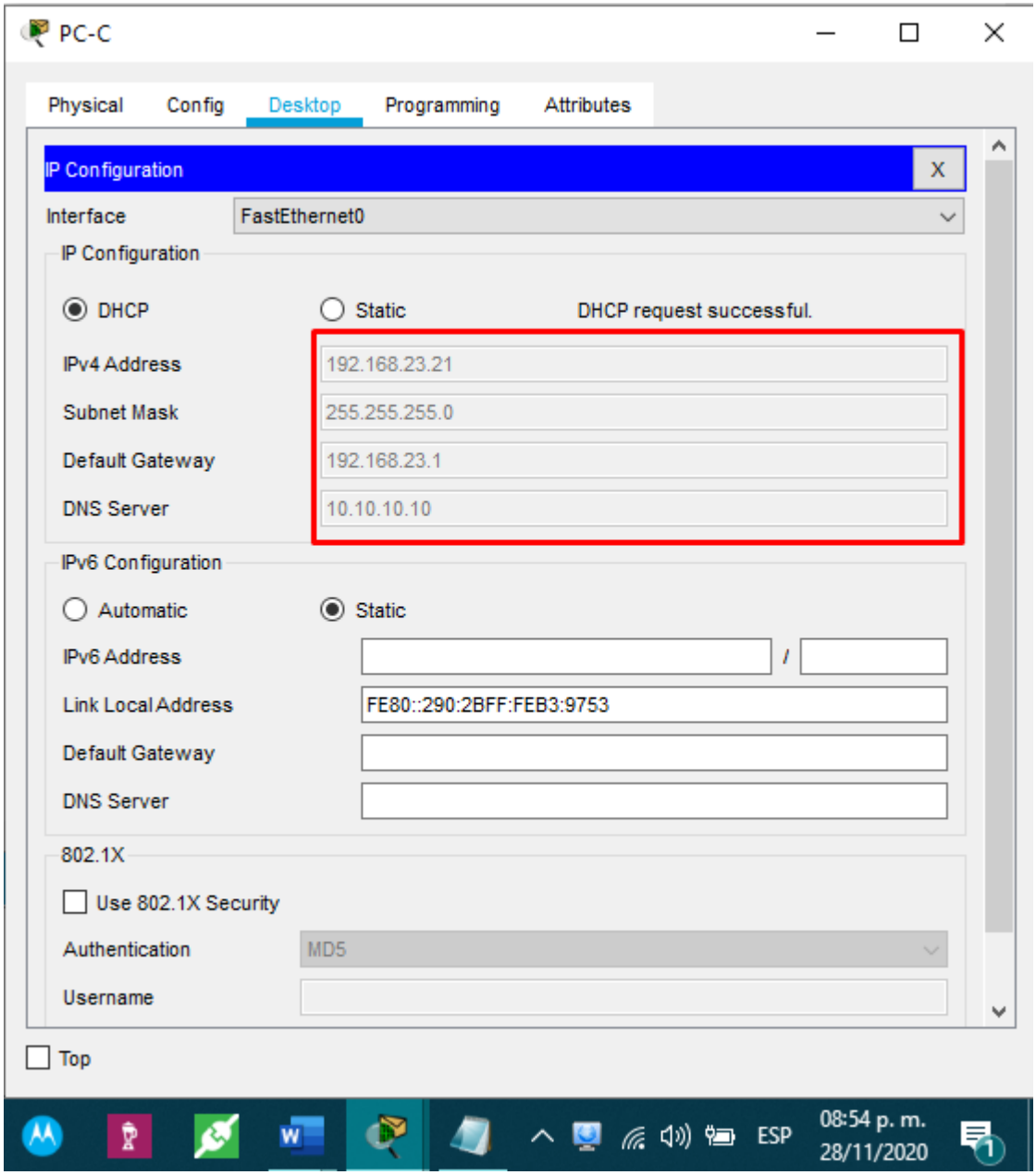
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	No se puede realizar la prueba por la incompatibilidad de los comandos con el software Cisco Packer Tracer.

Figura 52. Asignación de direccionamiento IP vía DHCP en PC-A.



Fuente: Autor

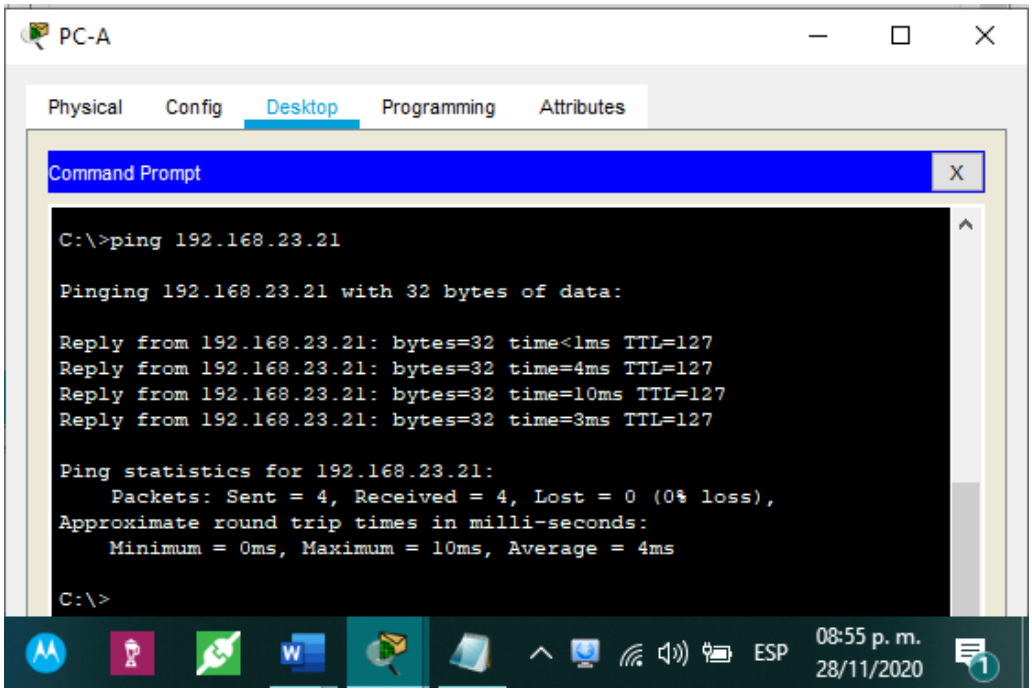
Figura 53. Asignación de direccionamiento IP vía DHCP en PC-C.



Fuente: Autor.

Cambiamos la configuración de direccionamiento IP de estático a dinámico (DHCP) de los clientes PC-A y PC-C para verificar el correcto funcionamiento del servidor DHCP.

Figura 54. Ping desde PC-A hacia PC-C.



Fuente: Autor.

Empleando el comando “ping” verificamos la conectividad entre los extremos de la red (PC-A y PC-C).

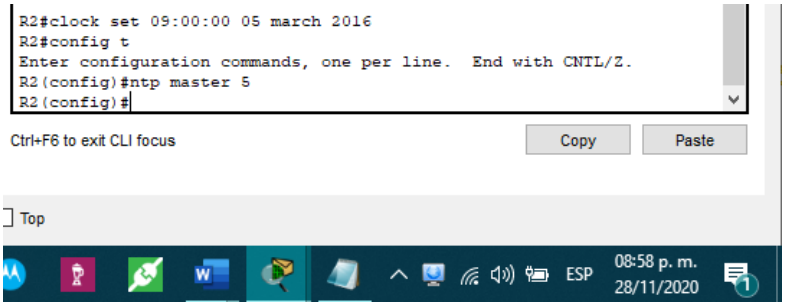
Configurar NTP

Tabla 32. Instrucciones y comandos de configuración NTP en R1 y R2.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	config t ntp master 5
Configurar R1 como un cliente NTP.	ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar

Verifique la configuración de NTP en R1.	show ntp associations

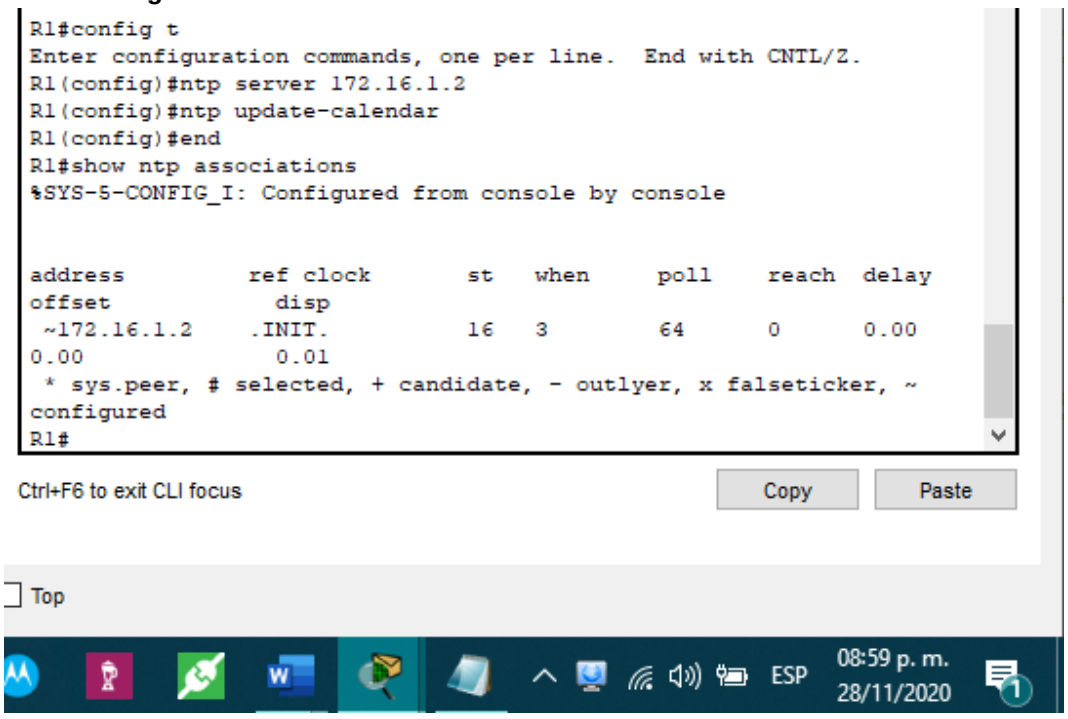
Figura 55. Configuración NTP en R2.



Fuente: Autor.

Empleando el comando “clock set” establecemos la fecha y hora para el enrutador R2. Configuramos R2 para que sea maestro NTP con el comando “ntp master 5”.

Figura 56. Configuración de cliente NTP en R1.



Fuente: Autor.

Configuramos el servidor NTP para R1 y actualizamos los datos con el comando “ntp update-calendar”. Verificamos las asociaciones NTP con el comando “show ntp associations”.

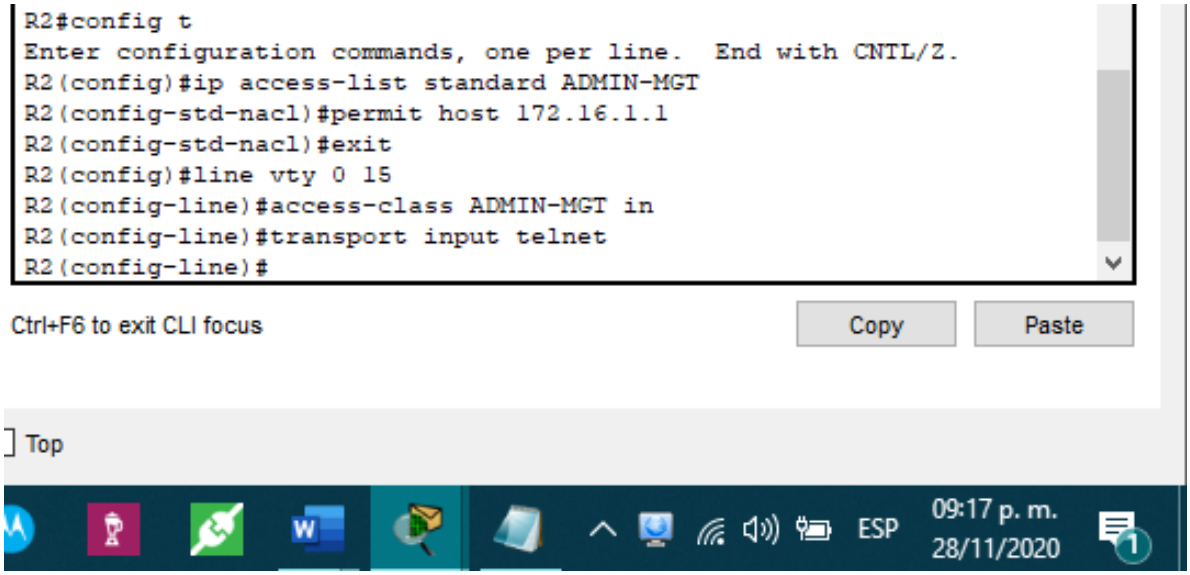
Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Tabla 33. Instrucciones y comandos de configuración de ACL en R2.

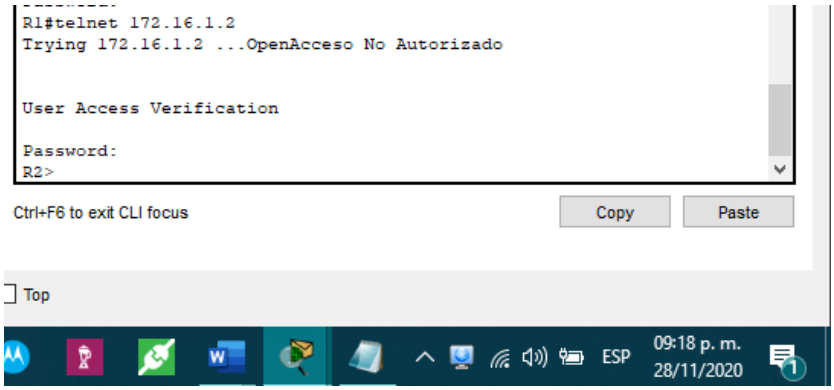
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	ip access-list standard ADMIN-MGT permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	Exitoso

Figura 57. Configuración de listas de control de acceso (ACL) en R2.



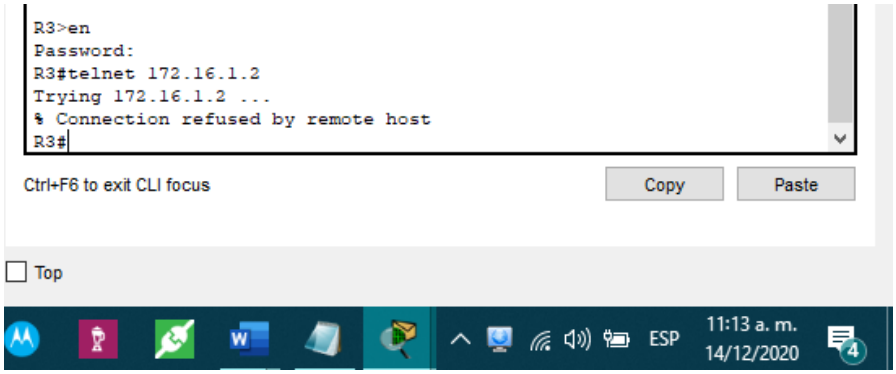
Fuente: Autor.

Figura 58. Acceso Telnet desde R1 hacia R2.



Fuente: Autor.

Figura 59. Acceso Telnet rechazado desde R3 hacia R2.



Fuente: Autor.

Verificamos el funcionamiento de la lista de control de acceso (ACL) obteniendo exitoso el proceso. Observamos como si permite la conexión Telnet desde R1 hacia R2 pero la conexión desde R3 hacia R2 es rechazada.

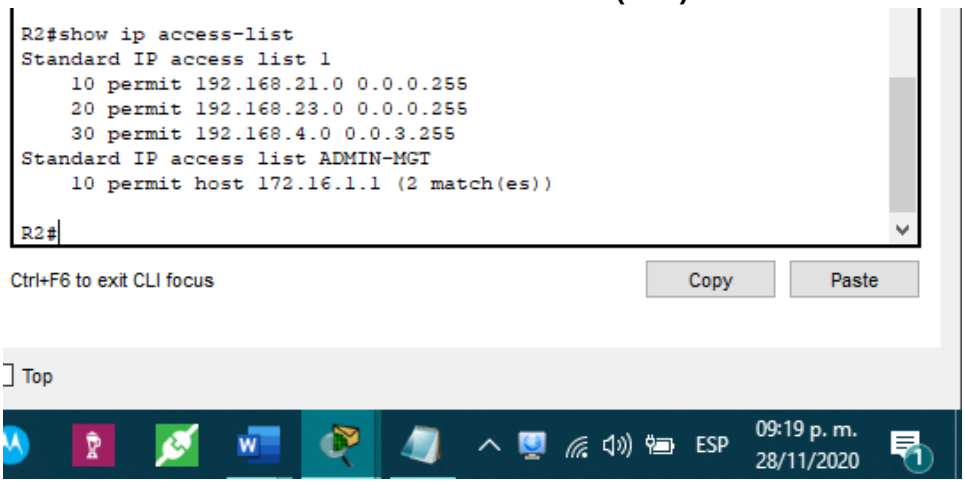
Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente:

Tabla 34. Verificación de ACL y traducciones NAT en R2.

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

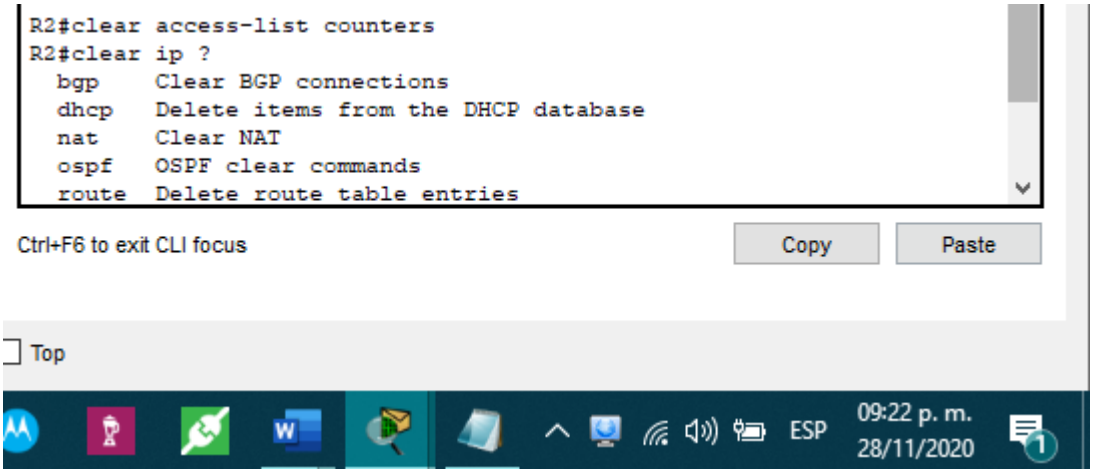
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip int
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translations

Figura 60. Verificación de las listas de control de acceso (ACL) en R2.



Fuente: Autor.

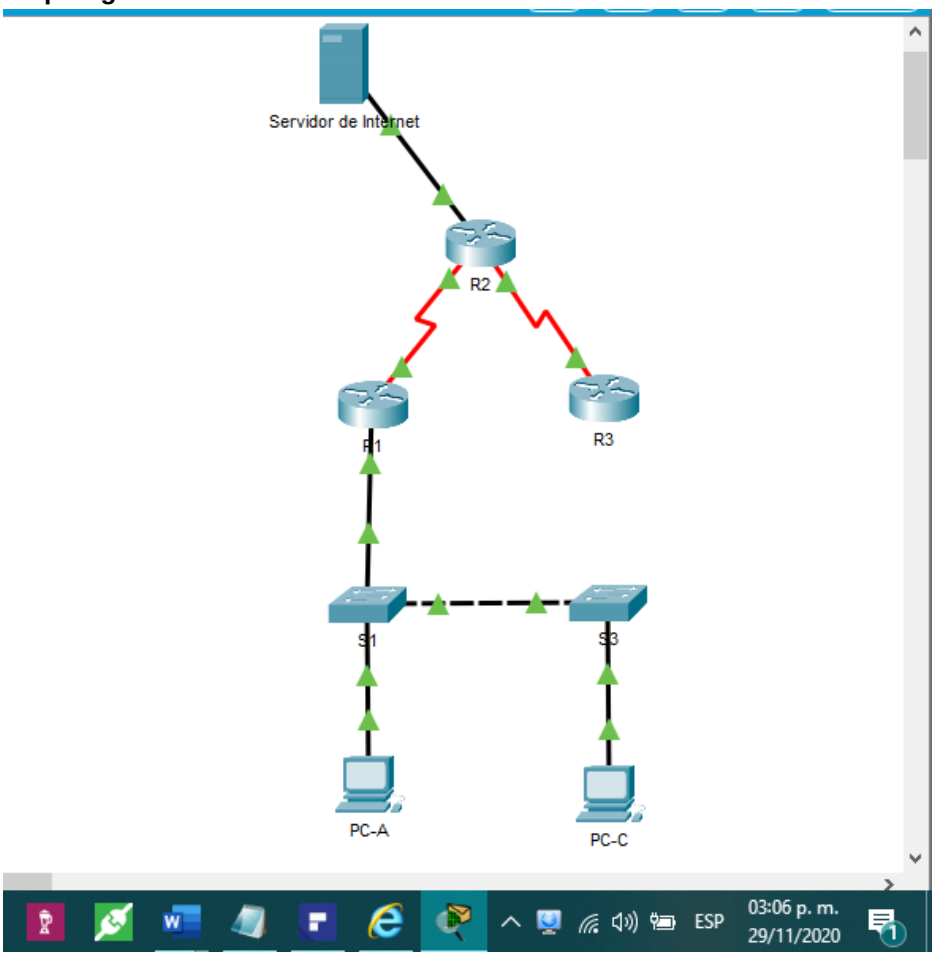
Figura 61. Restablecimiento de los contadores de la lista de control de acceso (ACL) en R2.



Fuente: Autor.

Utilizamos el comando “show ip Access-list” para visualizar las listas de control de acceso (ACL) y “clear Access-list counters” para restablecer los contadores de la lista de control de acceso (ACL).

Figura 62. Topología final de la red.



Fuente: Autor.

CONCLUSIONES

El desarrollo de prácticas de laboratorio utilizando el software Cisco Packet Tracer permite un aprendizaje avanzado en la configuración de los diferentes dispositivos de una red con equipamiento CISCO (switch, router, servidores, host) gracias a la simulación de “hardware” que permite una interacción segura y casi que realista con todos los dispositivos presentes en la biblioteca del software.

Hoy en día las empresas con visiones futuristas adoptan nuevas maneras de expandir sus servicios vía internet. Si no se implementa una seguridad adecuada el activo más importante de una empresa, la información, puede ser vulnerado a través de este medio. Es por esto que es de suma importancia que como administradores de la red nos apropiemos de técnicas de configuración de seguridad en los dispositivos que nos permitan garantizar la confiabilidad, integridad y disponibilidad de los recursos de la entidad.

La interfaz de línea de comando (CLI) esta basada en una estructura jerárquica. El software CISCO IOS realiza una división de las sesiones en diferentes niveles de acceso y por esto es de suma importancia tener claridad de lo anterior y comprender que cada modo de configuración permite una serie de comandos de configuración. La interfaz cuenta con un prompt para identificar de manera fácil en que modo estamos ubicados e ingresando los comandos.

Los routers y switches Cisco IOS comparten sistemas operativos modales y estructurales con una estructura de comando muy similar, es por esto que la configuración de parámetros básicos para su implementación en una red resulta casi que idénticos en ambos dispositivos.

Basado en la tabla de routing y en el protocolo de enrutamiento implementado un router elige la mejor ruta de en función del valor o la métrica que calcula para determinar la distancia para llegar al destino. Los protocolos dinámicos como RIP, OSPF y EIGRP haciendo uso de sus reglas y métricas realizan un cálculo para así elaborar y actualizar las tablas de routing, contrario al routing estático en el cual manualmente son ingresadas todas las rutas para la construcción de las tablas.

BIBLIOGRAFÍA

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

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

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

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). 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

ANEXOS

Link de descarga de archivos anexos:

PKT Escenario 1:
https://drive.google.com/file/d/1Fa26ReFuTEi6S4YfYXT3bBRUv25IHRwE/view?usp=sharing

PKT Escenario 2:
https://drive.google.com/file/d/1qfk5c3WdHIwH_uKhXfPpLVjfJFfP7sdr/view?usp=sharing

Desarrollo y verificación de conectividad en escenario propuesto empleando tecnología CISCO

Nicolas García Bonilla
Universidad Nacional Abierta y a Distancia - UNAD, ngarciabo@unadvirtual.edu.co

Resumen

Para este escenario se plantea una topología de red que incluye dispositivos capa 3, capa 2 y host como componentes de las capas de núcleo, distribución y acceso respectivamente. Para el desarrollo de los ítems propuestos se realizará la configuración de direccionamiento IPv4 e IPv6 en los dispositivos de la red, configuración de los parámetros básicos y de seguridad en routers y switches, se establecerá un correcto enrutamiento y servidores DHCP para las Vlan y además se configurarán los grupos de puertos EtherChannel y seguridad de los mismos.

Palabras clave: Enrutamiento, Router, Switch, Vlan, EtherChannel, Topología.

Abstract:

For this scenario, a network topology is proposed that includes layer 3, layer 2 and host devices as components of the core, distribution and access layers respectively. For the development of the proposed items, the IPv4 and IPv6 addressing configuration will be carried out in the network devices, configuration of the basic and security parameters in routers and switches, a correct routing and DHCP servers will be established for the Vlan and also they will configure the EtherChannel port groups and their security.

Keywords: Routing, Router, Switch, Vlan, EtherChannel, Topology.

I. INTRODUCCIÓN

Podemos definir una red como un conjunto de dispositivos conectados entre sí, que pueden comunicarse y compartir datos omitiendo la localización fisica de los distintos componentes. Dentro de estas redes nos topamos con un tipo en especial denominado LAN (Local Area Network) o red de área local, que presenta como principal caracteristica una extensión reducida o limitada y que son las más comunes en una oficina o edificio.

A medida que esta red LAN aumente su tamaño o requiera segmentación se hace necesario determinar una nueva arquitectura que garantice la escalabilidad, seguridad y gestión de red. Es aquí donde se emplean las Vlan (Virtual Local Area Network) o red de área local virtual. Las Vlan representan una gran alternativa ya que tienen una serie de características que resultan bastante útiles a la hora de la implementación de una red. Los principales beneficios a la hora de implementar Vlan's es su seguridad, mejora del rendimiento, simplicidad en su administración y la reducción en los costos de las implementaciones.

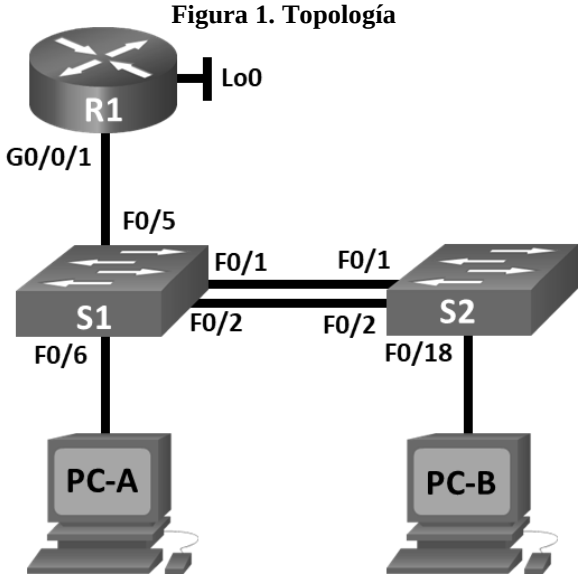
Para el escenario propuesto y a tratar en este artículo se configurarán los dispositivos capa 2 y capa 3 para garantizar un tráfico de datos correcto entre los dispositivos conectados en los extremos de la red LAN, implementando un enrutamiento entre redes virtuales (Vlan) y creando grupos de EtherChannel entre los conmutadores.

II. ESCENARIO I

A. Descripción

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 1. Topología



Fuente: Repositorio UNAD.

B. Definición de VLAN y Direccionamiento IP

Una vez definida la topología de red y el equipamiento hardware a usar es necesario establecer de manera ordenada la segmentación y el direccionamiento que van a ser configurados en las interfaces de red.

Tabla 1. Tabla de VLAN.

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 2. Direccionamiento IPv4 e IPv6.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

En la tabla 1 y tabla 2 se nos suministra toda la información referente a direccionamiento IP y VLAN para la configuración de las interfaces y dispositivos de la red el escenario planteado.

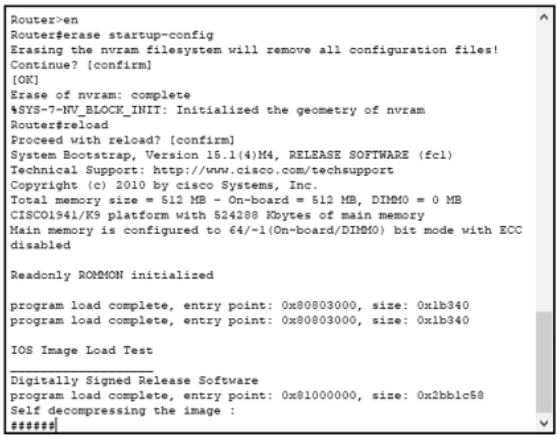
Configuración de dispositivos de red

Tabla 3. Instrucciones y comandos de configuración para inicializar y volver a cargar los dispositivos de red.

Tarea	*Especificación*
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***

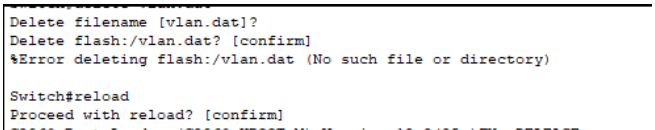
Al iniciar con la configuración de algún dispisitivo CISCO es escencial restablecer sus configuraciones por defecto. Para esto se borran las configuraciones de inicio y bases de datos VLAN para empezar con una configuración limpia y sin errores.

Figura 2. Eliminación de configuraciones de inicio y reinicio en enrutador CISCO.



Fuente: Autor.

Figura 3. Eliminación de tabla de VLAN en conmutador CISCO.



Fuente: Autor.

Tabla 4. Configuración de la plantilla SDM en S1 y S2.

Tarea	*Especificación*
Configurar la plantella SDM	***sdm prefer dual-ipv4-and-ipv6 default***
Volver a cargar el dispositivo	***reload***

Para habilitar el soporte IPv6 en los conmutadores S1 y S2 del escenario es necesario habilitar la plantilla SDM correspondiente. Hay que reiniciar el dispositivo para que la carga de la plantilla sea exitosa.

Tabla 5. Instrucciones y comandos para configuración básica y de interfaces en R1.

Tarea	Especificación
Desactivar la búsqueda DNS	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 secret ciscoenpass
Contraseña de acceso a la consola	line con 0 password ciscoconpass exit
Establecer la longitud mínima para las contraseñas	security passwords min-length 10
Crear un usuario administrativo en la base de datos local	username admin privilege 1 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 4 login local exit
Configurar VTY solo aceptando SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configure un MOTD Banner	banner motd #Solo operar personal autorizado#
Habilitar el routing IPv6	ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	int gi0/1 description LAN R1,S1 int gi0/1.2 description Bikes encapsulation dot1q 2 ip address 10.19.8.1 255.255.255.192 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:a::1/64 exit int gi0/1.3 description Trikes encapsulation dot1q 3 ip address 10.19.8.65 255.255.255.224 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:b::1/64 exit int gi0/1.4 description Management encapsulation dot1q 4 ip address 10.19.8.97 255.255.255.248 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:c::1/64 exit int gi0/1 no shutdown exit
Configure el Loopback0 interface	int loopback0 description LOOPBACK ip address 209.165.201.1 255.255.255.224 ipv6 address fe80::1 link-local ipv6 address 2001:db8:acad:209::1/64 exit
Generar una clave de cifrado RSA	crypto key generate rsa general-keys modulus 1024

Para la configuración básica de dispositivos se establecen los parámetros mas relevantes para la seguridad y administración del mismo. Es necesario determinar un nombre, un dominio, contraseñas para modos de usuario y lineas de acceso, además de encriptar las contraseñas de texto no cifrado y generar un banner de advertencia para personal sin aurotización de operar los dispositivos.

Figura 4. Configuración básica Router Cisco.

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin privilege 1 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Solo operar personal autorizado#
R1(config)#ipv6 unicast-routing
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com
```

Fuente: Autor.

Figura 5. Configuración de parámetros básicos en Conmutador Cisco.

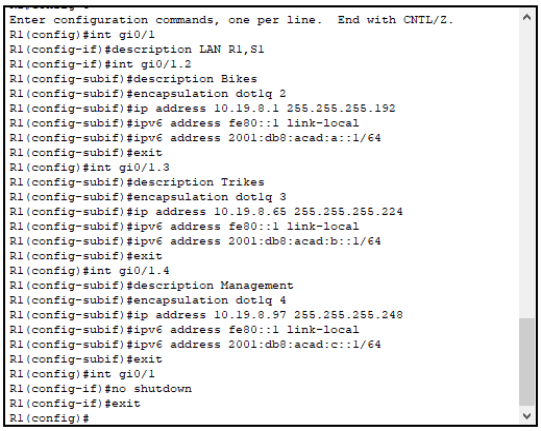
```
Switch>
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line con 0
S1(config-line)#password ciscoconpass
S1(config-line)#exit
S1(config)#username admin privilege 1 secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Solo operar personal autorizado#
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:5:37.966: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#ip defa
S1(config)#ip default-gateway 10.19.8.97
S1(config)#
```

Fuente: Autor.

Existen multiples tipos de interfaces en enrutatores y conmutadores CISCO. Para la conectividad entre estos es necesario designar un direccionamiento IP a cada una de ellas al igual que una descripción para la gestión y habilitarlas para que se genere el tráfico por ellas.

Figura 6. Configuración de interfaces en un Router CISCO.



```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gi0/1
R1(config-if)#description LAN R1,S1
R1(config-if)#int gi0/1.2
R1(config-subif)#description Bikes
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#exit
R1(config)#int gi0/1.3
R1(config-subif)#description Trikes
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#exit
R1(config)#int gi0/1.4
R1(config-subif)#description Management
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#exit
R1(config)#int gi0/1
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

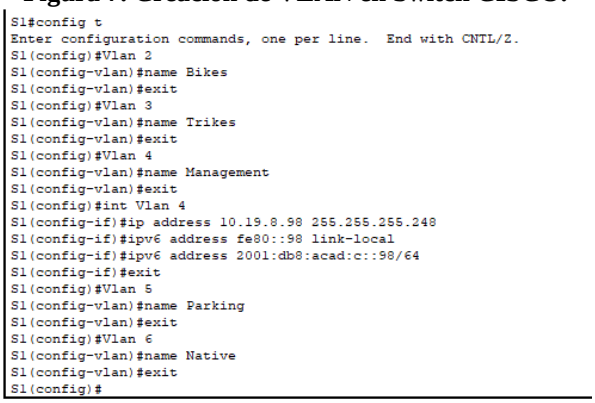
Fuente: Autor.

Tabla 6. Intrucciones y comandos de configuración de la estructura de red en Conmutador Cisco.

Tarea	Especificación
Crear VLAN	Vlan 2 name Bikes exit Vlan 3 name Trikes exit Vlan 4 name Management exit int Vlan 4 ip address 10.19.8.98 255.255.255.248 ipv6 address fe80::98 link-local ipv6 address 2001:db8:acad:c::98/64 exit Vlan 5 name Parking exit Vlan 6 name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	int f0/1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 exit int f0/5 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	int range f0/1-2 channel-group 1 mode active int port-channel 1 switchport mode trunk switchport trunk allowed vlan all
Configurar el puerto de acceso de host para VLAN 2	int f0/6 switchport mode access switchport access vlan 2
Configurar el puerto de acceso de host para VLAN 2	int f0/6 switchport mode access switchport access vlan 2
Configurar el puerto de acceso de host para VLAN 2	int f0/6 switchport mode access switchport access vlan 2

Una VLAN se puede configurar de varias formas y una de ellas es a través de los puertos fisicos. Una vez creadas las VLAN podemos establecer que puerto pertenece a cada una de ellas y así segmentar el tráfico de la red. Para transportar varias VLAN por un puerto fisico de un conmutador a otro es necesario establecer enlaces troncales y protocolos de agrupación lógica de puertos fisicos EtherChannel.

Figura 7. Creación de VLAN en Switch CISCO.



```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#Vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#exit
S1(config)#Vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#exit
S1(config)#Vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#int Vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#exit
S1(config)#Vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#exit
S1(config)#Vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#
```

Fuente: Autor.

Figura 8. Configuración de enlaces Troncales y EthcrChannel en Switch CISCO.

```
S2(config)#int f0/2
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#int f0/5
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#int range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#int port-channel 1
S2(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto"
can not be configured to "trunk" mode.
S2(config-if)#switchport trunk allowed vlan all
S2(config-if)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security maximum 3
S2(config-if)#int range f0/3-17, f0/19-24
S2(config-if-range)#description Parking
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#shut
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
```

Fuente: Autor.

Tabla 7. Instrucciones y comandos de configuración para la creación de una ruta estática predeterminada.

Tarea	Especificación
Configure Default Routing	ip route 0.0.0.0 0.0.0.0 Loopback0 ipv6 route ::/0 Loopback0

Cuando se realiza la configuración del enrutamiento en una red local, es de vital importancia conocer que tipo se va a emplear. Existen 3 tipos de routing: Estático, Dinámico y Combinado. Para este escenario se plantea utilizar una ruta predeterminada estática que tiene como finalidad coincidir con todos los paquetes que circulan por la red.

Figura 9. Creación de ruta estática predeterminada en Enrutador Cisco.

```
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback0
R1(config)#ipv6 route ::/0 Loopback0
R1(config)#
```

Fuente: Autor.

Tabla 8. Instrucciones y comandos de configuración para soporte de Host en Enrutador Cisco.

Tarea	Especificación
Configurar IPv4 DHCP para VLAN 2	ip dhcp pool Bikes network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 exit ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	ip dhcp pool Trikes network 10.19.8.64 255.255.255.224 default-router 10.19.8.65 exit ip dhcp excluded-address 10.19.8.65 10.19.8.84

Las direcciones IP pueden ser asignadas a un dispositivo de manera estatica (manualmente) o dinamicamente (DHCP) segú sea el caso. Para un asigación dinamica se requiere de un dispositivo en la red que preste el servicio DHCP en los segmentos requeridos. Es necesario configurar este servicio para que asigne no solo la dirección IP sino tambien la máscara de red, el Gateway y el servidor DNS.

Figura 10. Configuración de Router CISCO como servidor DHCP para 2 segmentos de red.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#
R1(config)#ip dhcp pool Trikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#
```

Fuente: Autor.

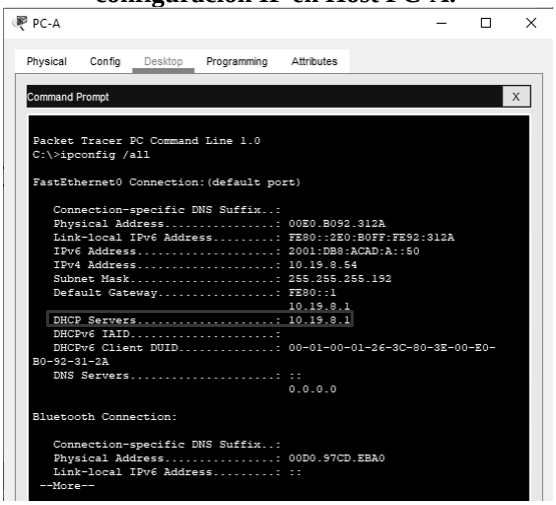
Tabla 9. Configuración de direccionamiento IP PC-A.

PC-A Network Configuration	
Descripción	FastEthernet0
Dirección física	00E0:B092:312A
Dirección IP	DHCP IPv4 2001:DB8:ACAD:A::50
Máscara de subred	DHCP IPv4
Gateway predeterminado	DHCP IPv4
Gateway predeterminado IPv6	FE80::1

Tabla 10. Configuración de direccionamiento IP PC-B.

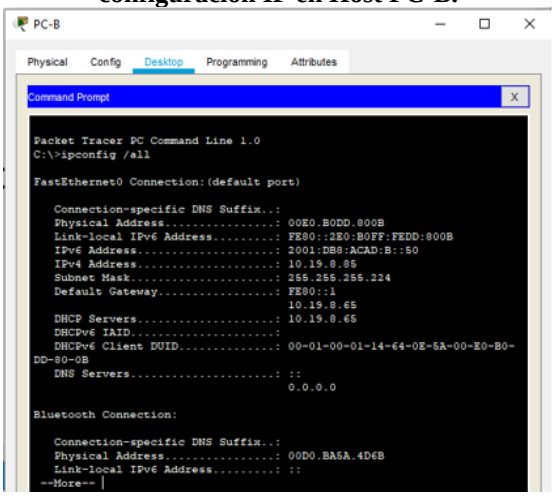
PC-B Network Configuration	
Descripción	Fastethernet0
Dirección física	00E0:B0DD:800B
Dirección IP	10.19.8.85 2001.DB8:ACAD:B::50
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 11. Funcionamiento de servicio DHCP y configuración IP en Host PC-A.



Fuente: Autor.

Figura 12. Funcionamiento de servicio DHCP y configuración IP en Host PC-B.



Fuente: Autor.

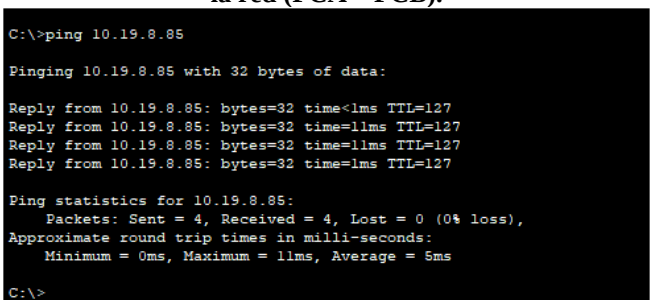
C. Pruebas de Conectividad

Para garantizar el correcto funcionamiento del enrutamiento de la red es necesario realizar pruebas de conexión entre los dispositivos ubicados en los extremos de la red. La prueba más sencilla y que tiene mas uso por administradores de la red es ejecutar el comando PING para probar la conectividad entre 2 dispositivos de la red. Este comando envía paquetes ICMP a la dirección de destino esperando obtener respuesta con paquetes de retorno ICPM tambien, esta respuesta es medida en unidades de tiempo y basados en esto se pueden diagnosticar problemas de conectividad.

Tabla 11. Instrucciones para verificación de conectividad de extremo a extremo de la red.

Desde	A	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	10.19.8.1	**OK**
PC-A	R1, G0/0/1.2	2001:db8:acad:a: :1	**OK**
PC-A	R1, G0/0/1.3	10.19.8.65	**OK**
PC-A	R1, G0/0/1.3	2001:db8:acad:b: :1	**OK**
PC-A	R1, G0/0/1.4	10.19.8.97	**OK**
PC-A	R1, G0/0/1.4	2001:db8:acad:c: :1	**OK**
PC-A	S1, VLAN 4	10.19.8.98	**OK**
PC-A	S1, VLAN 4	2001:db8:acad:c: :98	**OK**
PC-A	S2, VLAN 4	10.19.8.99.	**OK**
PC-A	S2, VLAN 4	2001:db8:acad:c: :99	**OK**
PC-A	PC-B	10.19.8.85	**OK**
PC-A	PC-B	2001:db8:acad:b: :50	**OK**
PC-A	R1 Bucle 0	209.165.201.1	**OK**
PC-A	R1 Bucle 0	2001:db8:acad:209: :1	**OK**
PC-B	R1 Bucle 0	209.165.201.1	**OK**
PC-B	R1 Bucle 0	2001:db8:acad:209: :1	**OK**
PC-B	R1, G0/0/1.2	10.19.8.1	**OK**
PC-B	R1, G0/0/1.2	2001:db8:acad:a: :1	**OK**
PC-B	R1, G0/0/1.3	10.19.8.65	**OK**
PC-B	R1, G0/0/1.3	2001:db8:acad:b: :1	**OK**
PC-B	R1, G0/0/1.4	10.19.8.97	**OK**
PC-B	R1, G0/0/1.4	2001:db8:acad:c: :1	**OK**
PC-B	S1, VLAN 4	10.19.8.98	**OK**
PC-B	S1, VLAN 4	2001:db8:acad:c: :98	**OK**
PC-B	S2, VLAN 4	10.19.8.99	**OK**
PC-B	S2, VLAN 4	2001:db8:acad:c: :99	**OK**

Figura 13. Respuesta al comando Ping entre extremos de la red (PCA – PCB).



Fuente: Autor.

III. CONCLUSIONES

La seguridad de las redes es un aspecto a considerar y que está tomando relevancia ya que cada vez son más los datos que manejamos por medio de nuestros equipos de red. La exposición a factores como robo de información y de identidad, perdida o manipulación de datos e interrupción del servicio, nos crea la necesidad de cada vez implementar redes más seguras y confiables. Es por esto que es importante tener buenas prácticas de seguridad a la hora de configurar nuestros equipos y considerar la posibilidad de adquirir hardware como un firewall para garantizar un buen nivel de seguridad general de nuestra red.

Un factor importante en el desarrollo de una empresa es el rendimiento de su red. Por lo anterior los avances en las tecnologías y sus implementaciones han cobrado un valor relevante, es por esto que como administradores de red debemos de adoptar métodos que nos permitan garantizar la escalabilidad y funcionamiento de las redes. La implementación de VLAN es uno de estos ya que nos permite tener una mayor seguridad, fácil escalabilidad y gestión centralizada ya que podremos configurar todos los equipos en un entorno centralizado como lo observamos en el desarrollo del escenario.

IV. REFERENCIAS

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

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

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

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

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

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

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

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

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

[10] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

V. BIOGRAFÍA

Nicolas García Bonilla

Nacido en Ibagué (Tolima), el 4 de octubre de 1993.

Graduado como bachiller académico de la institución educativa Diego Fallón de la ciudad de Ibagué, realizó el curso de Mecatrónica en el servicio nacional de aprendizaje SENA, obteniendo varios galardones entre ellos el primer puesto en las olimpiadas nacionales de mecatrónica orquestadas por la multinacional FESTO.

Cuenta con experiencia laboral en campos como la metalmecánica, electrónica, programación y las telecomunicaciones. Ha participado en proyectos de integración IT desempeñando el cargo de líder técnico. Actualmente labora para la compañía Servicios y Comunicaciones SERVICOM SAS ocupando el cargo de Técnico Telemático a cargo de la administración del sistema de Radiocomunicaciones, Radio FM y sistemas PTP de la concesionaria vial COVIANDINA en el tramo de la vía Bogotá – Villavicencio.