SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

ONOFRE MEJÍA ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
COLOMBIA
2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

ONOFRE MEJÍA ROMERO

Diplomado de opción de grado presentado para optar el título de INGENIERÍA ELECTRÓNICA

DIRECTOR
JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
COLOMBIA
2020

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Florencia, 30 de Noviembre de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

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

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

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

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

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

INTERFAZ: Se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común. Se conoce como Interfaz Física a los medios utilizados para la conexión de un computador con el medio de transporte de la red.

RESUMEN

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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.

Para el segundo escenario, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente

PALABRAS CLAVE: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

ABSTRACT

The evaluation called "Test of practical skills" is part of the evaluative activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of skills and abilities that were acquired throughout the diploma. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

In this first scenario, the devices of a small network will be configured. You must configure a router, switch, and computers that support both IPv4 and IPv6 connectivity for the supported hosts. The router and switch must also be managed securely. You will configure routing between VLAN, DHCP, Etherchannel, and port-security.

For the second scenario, a small network must be configured to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), address translation dynamic and static network (NAT), access control lists (ACLs), and network time protocol (NTP) server / client

KEY WORDS: CISCO, Switching, Routing, Networks, Systems

1. INTRODUCCIÓN

Para esta actividad, se dispone de un tiempo para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

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. Para el segundo escenario, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, y demás configuraciones que contribuyen a la correcta solución del escenario.

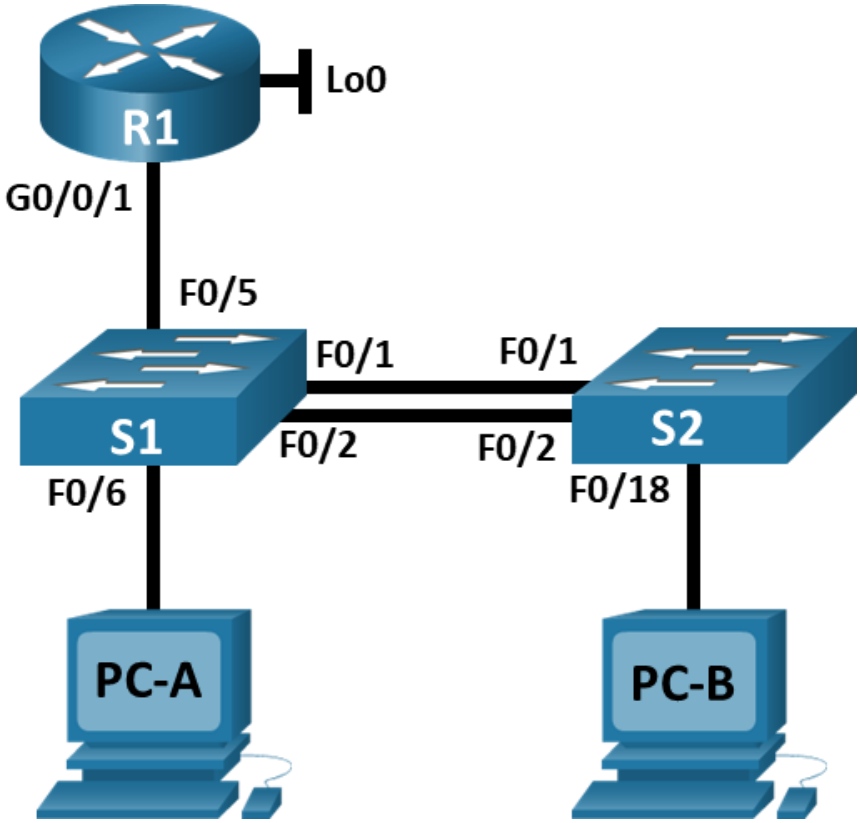
Al final, cada proceso está debidamente documentado y consta de una evidencia que determina la operación y aplicación de cada una de las instrucciones requeridas para el cumplimiento de lo solicitado en cada uno de los escenarios y además de verificar el funcionamiento y el comportamiento de la red a medida que se va implementando cada uno de los cambios y configuración de los dispositivos.

2. DESARROLLO DEL PROYECTO

2.1. Escenario 1

Topología

Figura 1. Topología del escenario 1



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.

Se construye el escenario utilizando la herramienta Packet Tracer, utilizando un router, dos switches y dos dispositivos finales.

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
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	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
	2001:db8:acad:c: :98 /64	No corresponde
	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
	2001:db8:acad:a: :50 /64	fe80::1

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

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

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: 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.

Router R1

Router>enable
Router#erase startup-config Se elimina la configuración de inicio
Router#reload Se reinicia el dispositivo

Switch S1

Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete

Switch#

Switch#reload

Proceed with reload? [confirm]

En S2

Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete

Switch#

Switch#reload

Proceed with reload? [confirm]

- 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.

Parte 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Tareas de configuración para el Router R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin privilege 15 secret admin1pass

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #El acceso no autorizado esta prohibido#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface gi0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN to VLAN2 R1(config-subif)#ip add 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#ip add 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN3 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gi0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#ip add 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN4 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gi0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#exit R1(config)#interface gi0/1 R1(config-if)#no shutdown

Tarea	Especificación
Configure el Loopback0 interface	R1(config)#interface lo0 R1(config-if)#description LAN to Loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add FE80::1 link-local R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa

En esta asignación, se crean las respectivas subinterfaces, encapsulándolas con su vlan y asignando el direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH.

Parte 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Configuración S1.

Tabla 4. Tareas de configuración para el Switch S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)# banner motd #El acceso no autorizado esta prohibido#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip add 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

Configuración S2.

Tabla 5. Tareas de configuración para el Switch S2

Tarea	Especificación
Desactivar la búsqueda DNS.	S2(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1

Tarea	Especificación
Nombre de dominio	S2(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line con 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #El acceso no autorizado esta prohibido#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip add 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit

Tarea	Especificación
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Tareas de configuración VLAN y troncales para el Switch S1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal S1(config)#interface fa0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1#configure terminal S1(config)#interface fa0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 2 mode active S1(config)#exit S1(config#interface port-channel 2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config)#switchport trunk native vlan 6

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#interface fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Puertos sin utilizar S1(config-if-range)#shutdown

Paso 2: Configure el S2.

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

Tabla 7. Tareas de configuración VLAN y troncales para el Switch S2

Parte 2: Configurar soporte de hostTarea	**Especificación**
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native

Parte 2: Configurar soporte de hostTarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface port S2(config)#interface port-channel 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)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	S2(config)#interface fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3

Parte 2: Configurar soporte de hostTarea	Especificación
Asegure todas las interfaces no utilizadas.	S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Puertos no utilizados S2(config-if-range)#shutdown

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Tareas de configuración DHCP Router R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
Configurar IPv4 DHCP para VLAN 2	R1#configure terminal R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name CCNA-a.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.2 10.19.8.51

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name CCNA-b.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.66 10.19.8.83

Paso 2: 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 9. Configuración PC-A DHCP

PC-A Network Configuration	
Descripción	CCNA-a.net
Dirección física	0000.0C89.3578
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 10. Configuración PC-B DHCP

Configuración de red de PC-B	
Descripción	CCNA-b.net
Dirección física	00D0.BCDC.3ADB
Dirección IP	10.19.8.84
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Parte 3. 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 11. Verificación de las configuraciones y conectividad extremo a extremo

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

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.2	Dirección	10.19.8.1	
		IPv6	2001:db8:acad:a: :1	
	R1, G0/0/1.3	Dirección	10.19.8.65	
		IPv6	2001:db8:acad:b: :1	
	R1, G0/0/1.4	Dirección	10.19.8.97	
		IPv6	2001:db8:acad:c: :1	
	S1, VLAN 4	Dirección	10.19.8.98	
		IPv6	2001:db8:acad:c: :98	
	S2, VLAN 4	Dirección	10.19.8.99.	
		IPv6	2001:db8:acad:c: :99	

PC-A

R1, G0/0/1.2

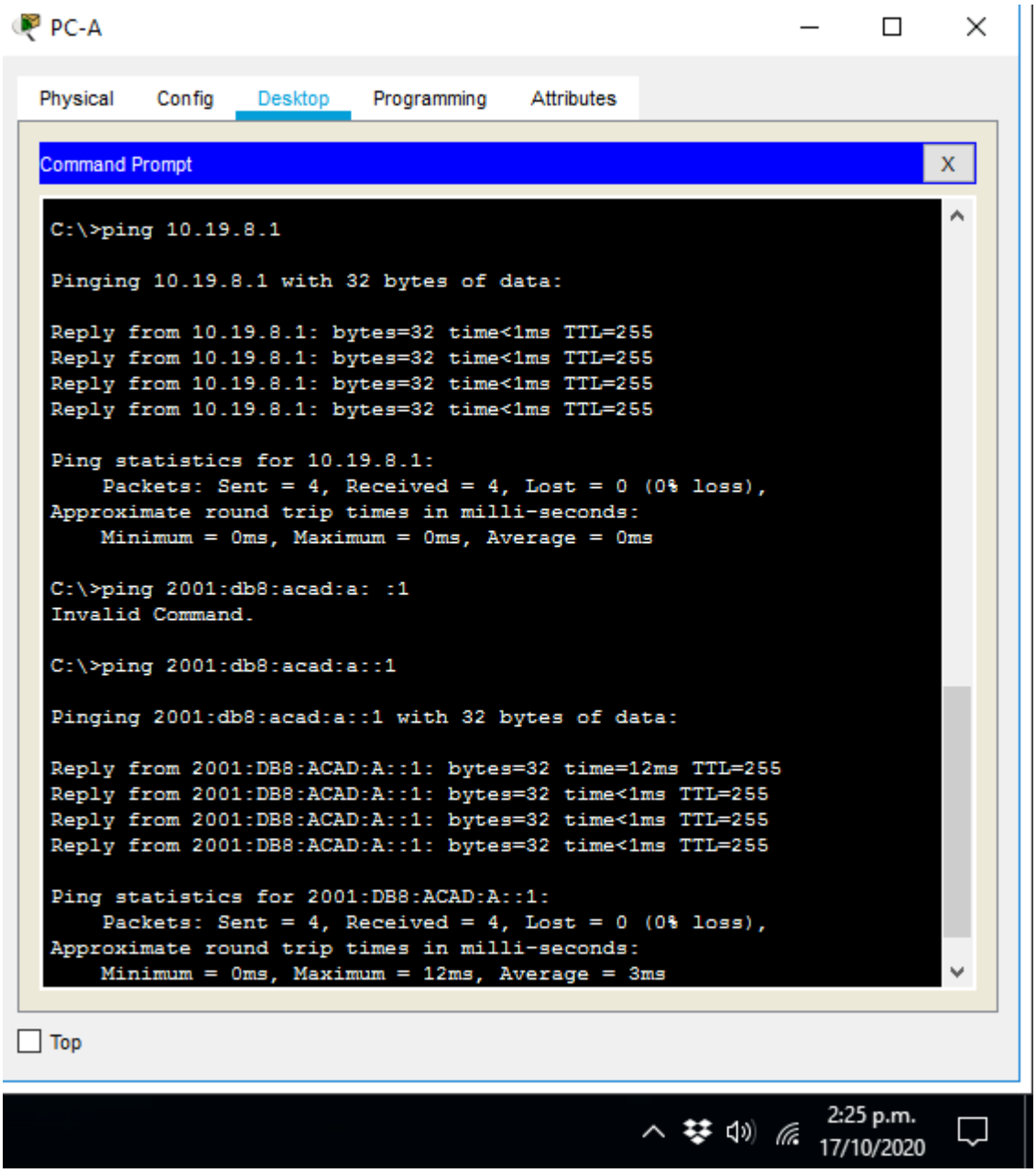


Figura 2. Ping de PC-A a R1 G0/0/1.2.

R1, G0/0/1.3

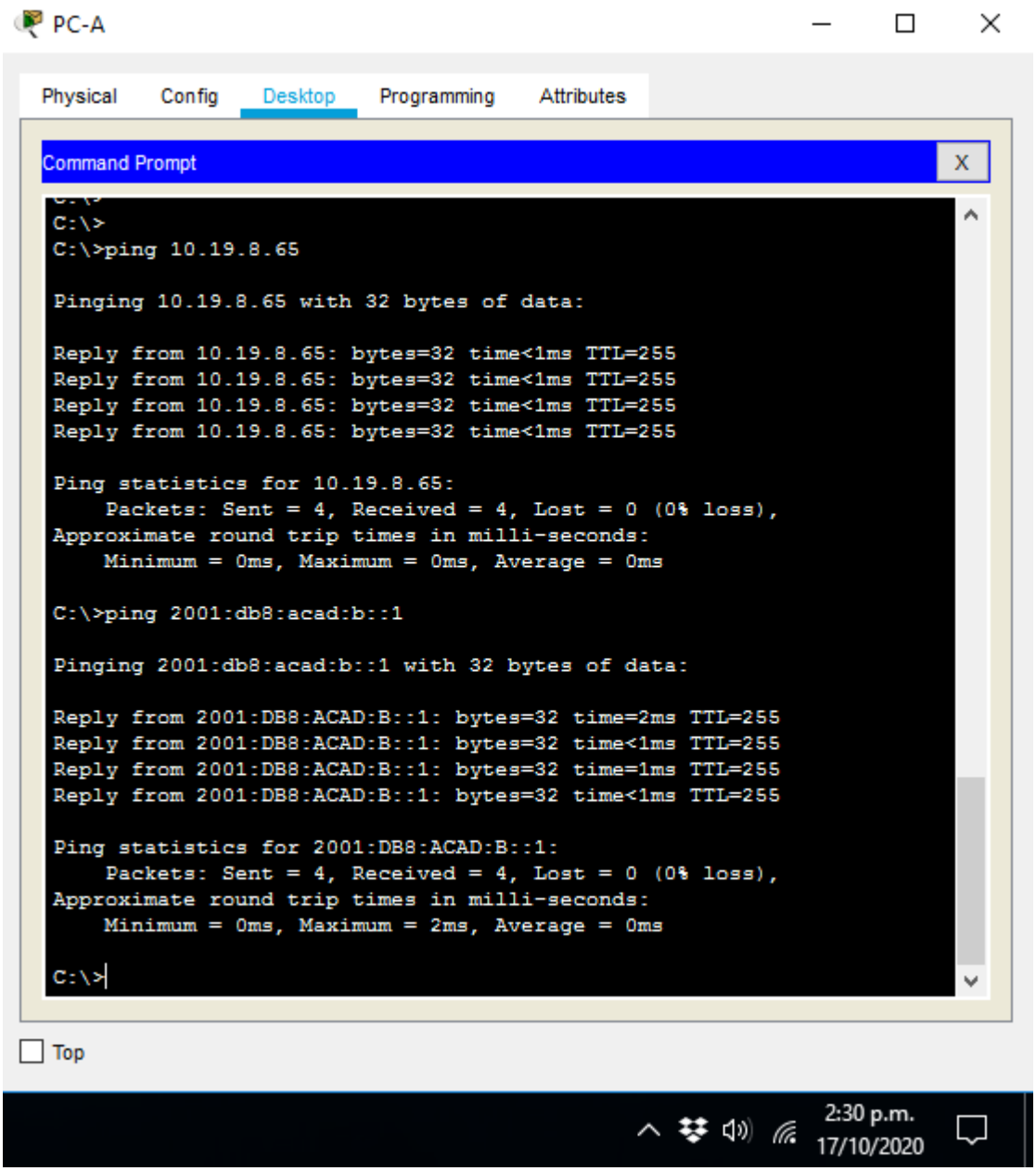


Figura 3. Ping de PC-A a R1 G0/0/1.3.

R1, G0/0/1.4

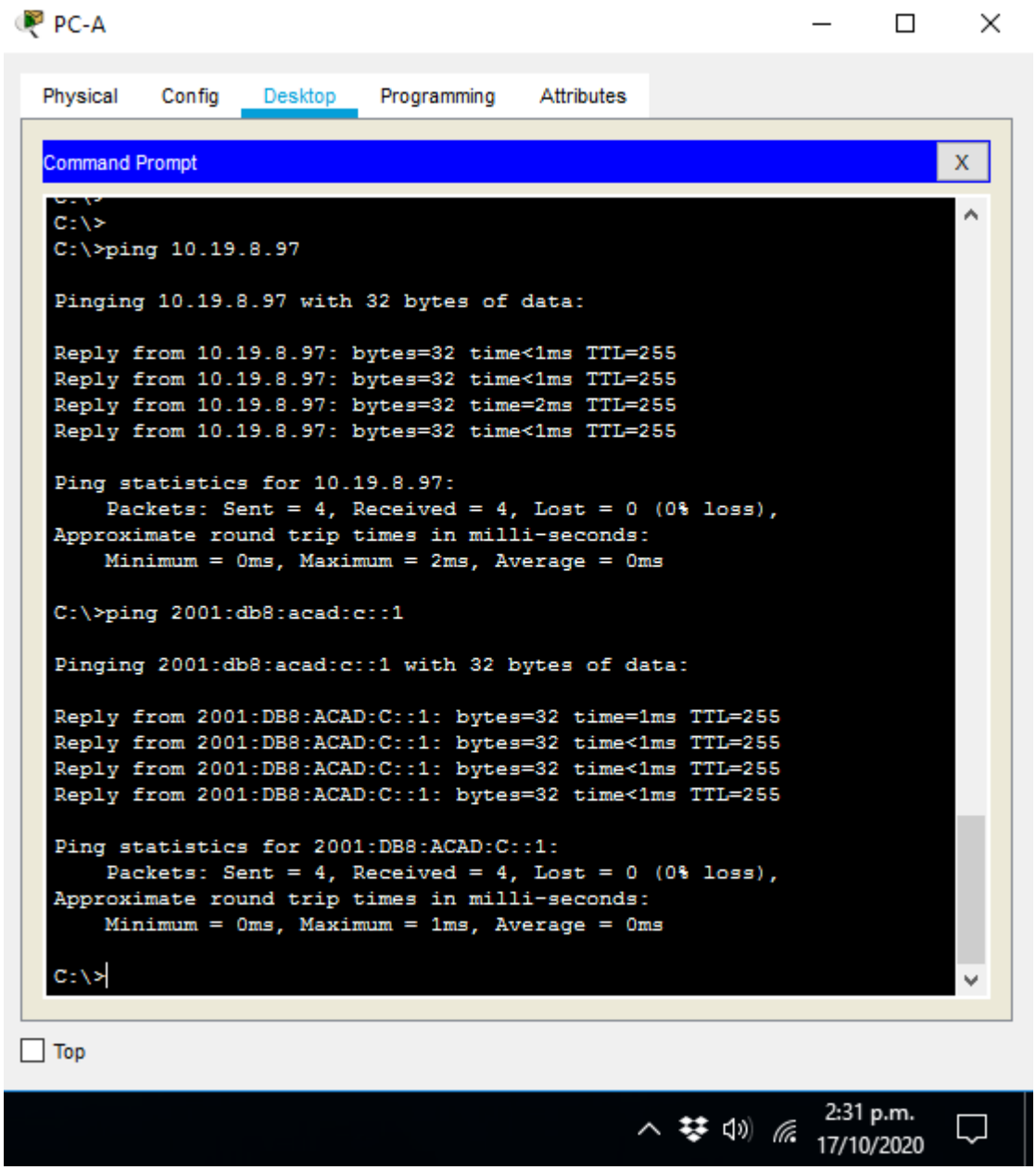


Figura 4. Ping de PC-A a R1 G0/0/1.4.

S1, VLAN 4

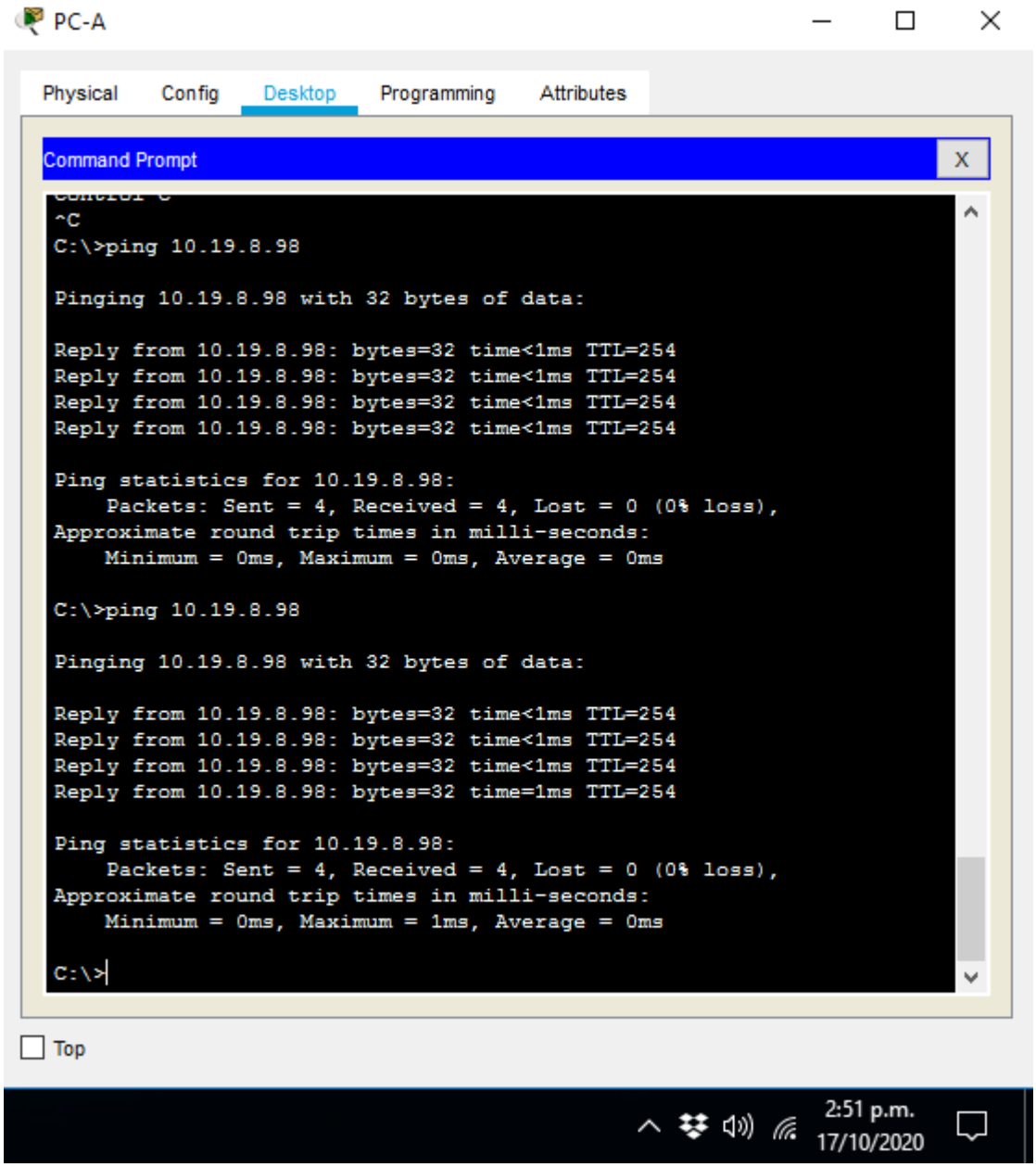


Figura 5. Ping de PC-A a S1 VLAN 4.

S2, VLAN 4

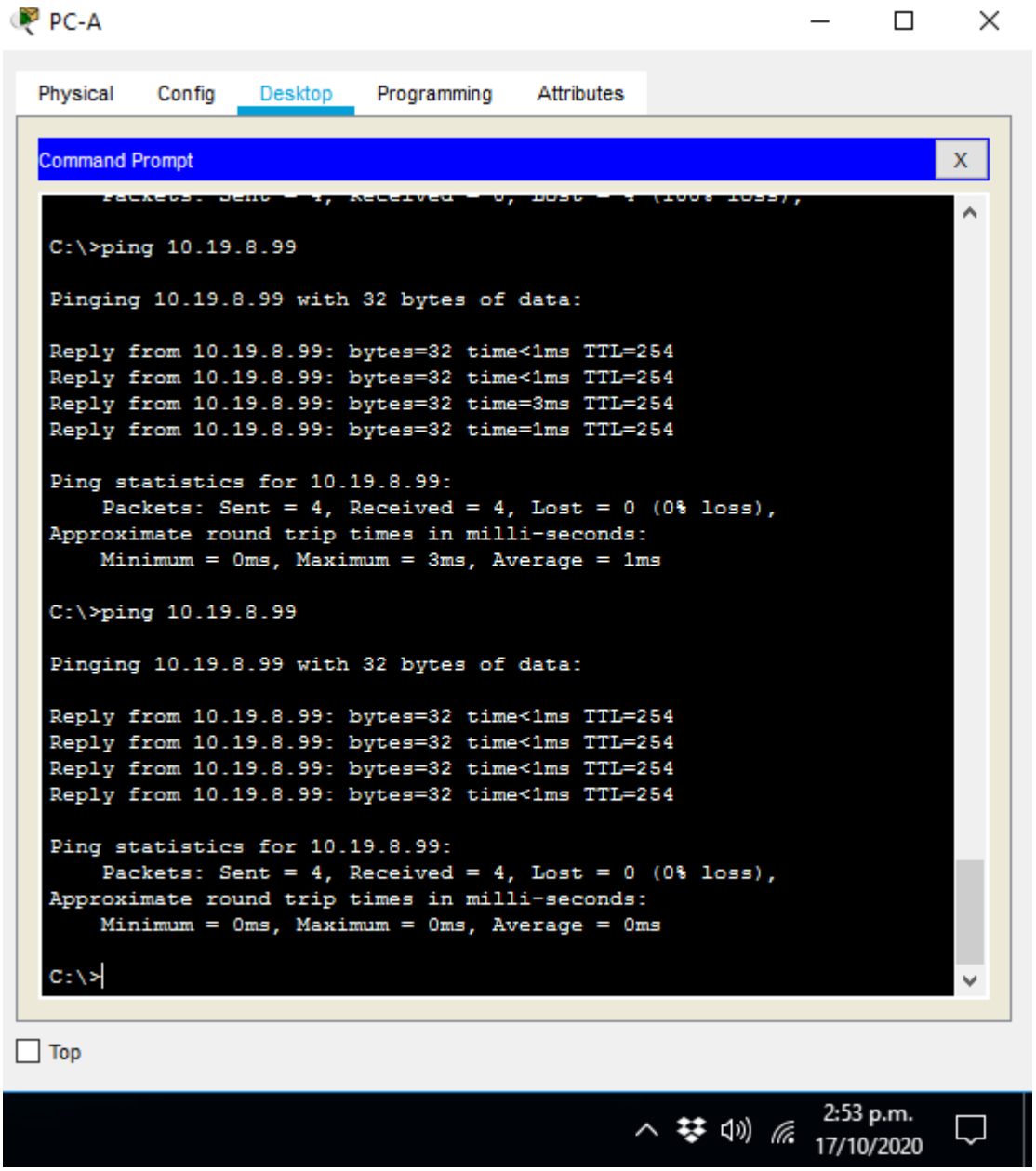


Figura 6. Ping de PC-A a S2 VLAN 4.

PC-B

R1 Bucle 0

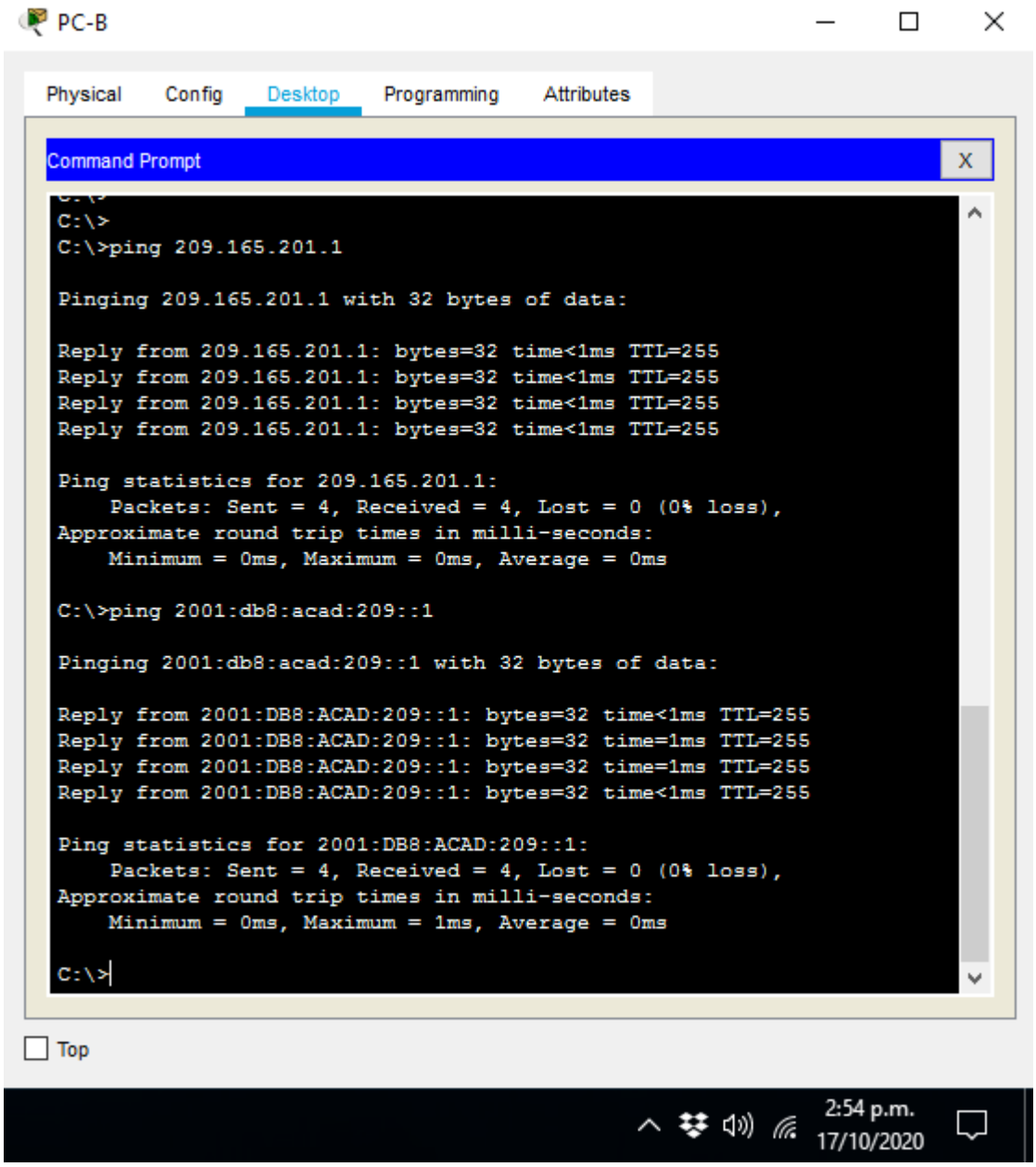


Figura 7. Ping de PC-B a R1 Bucle 0.

R1, G0/0/1.2

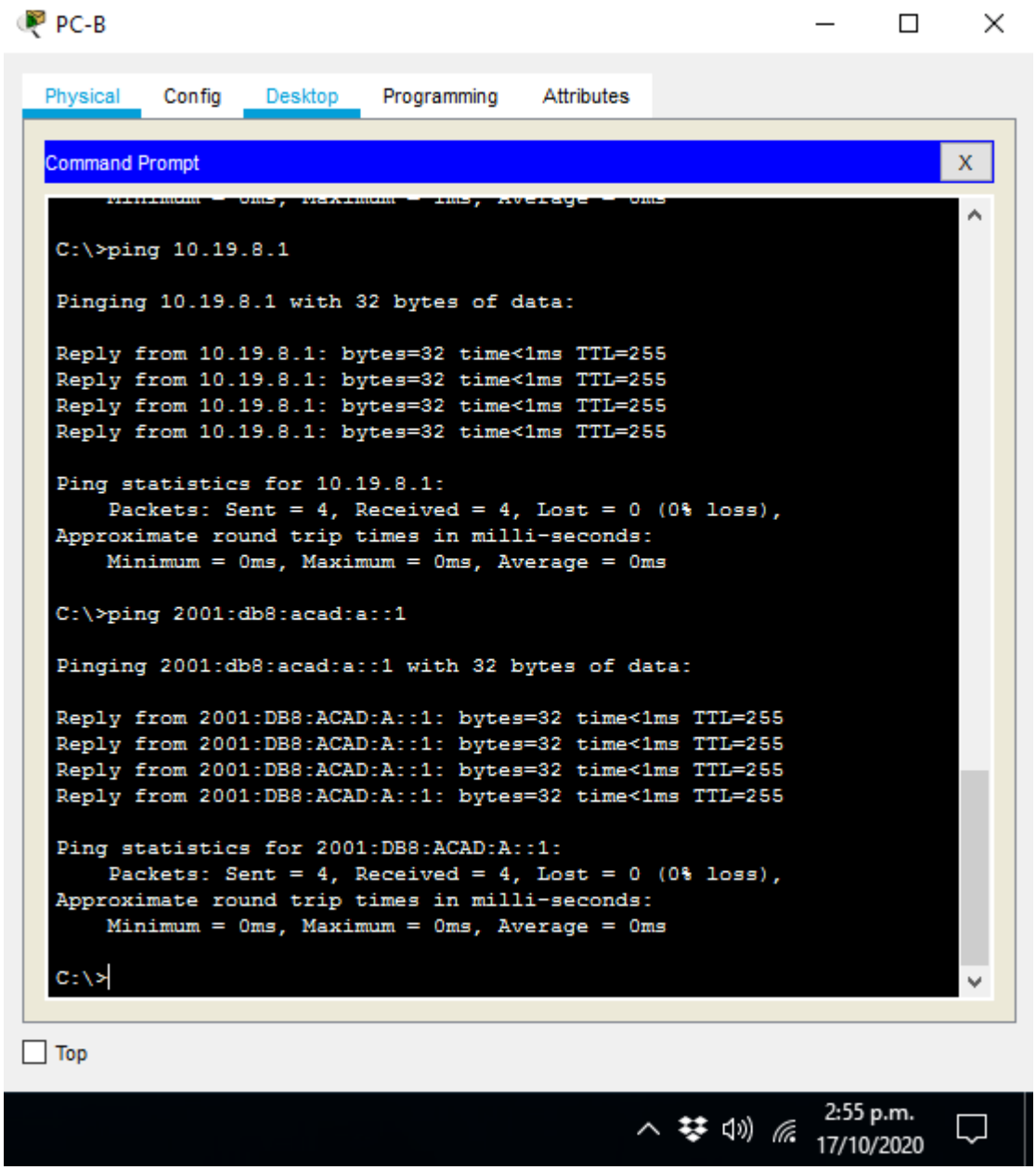


Figura 8. Ping de PC-B a R1 G0/0/1.2.

R1, G0/0/1.3

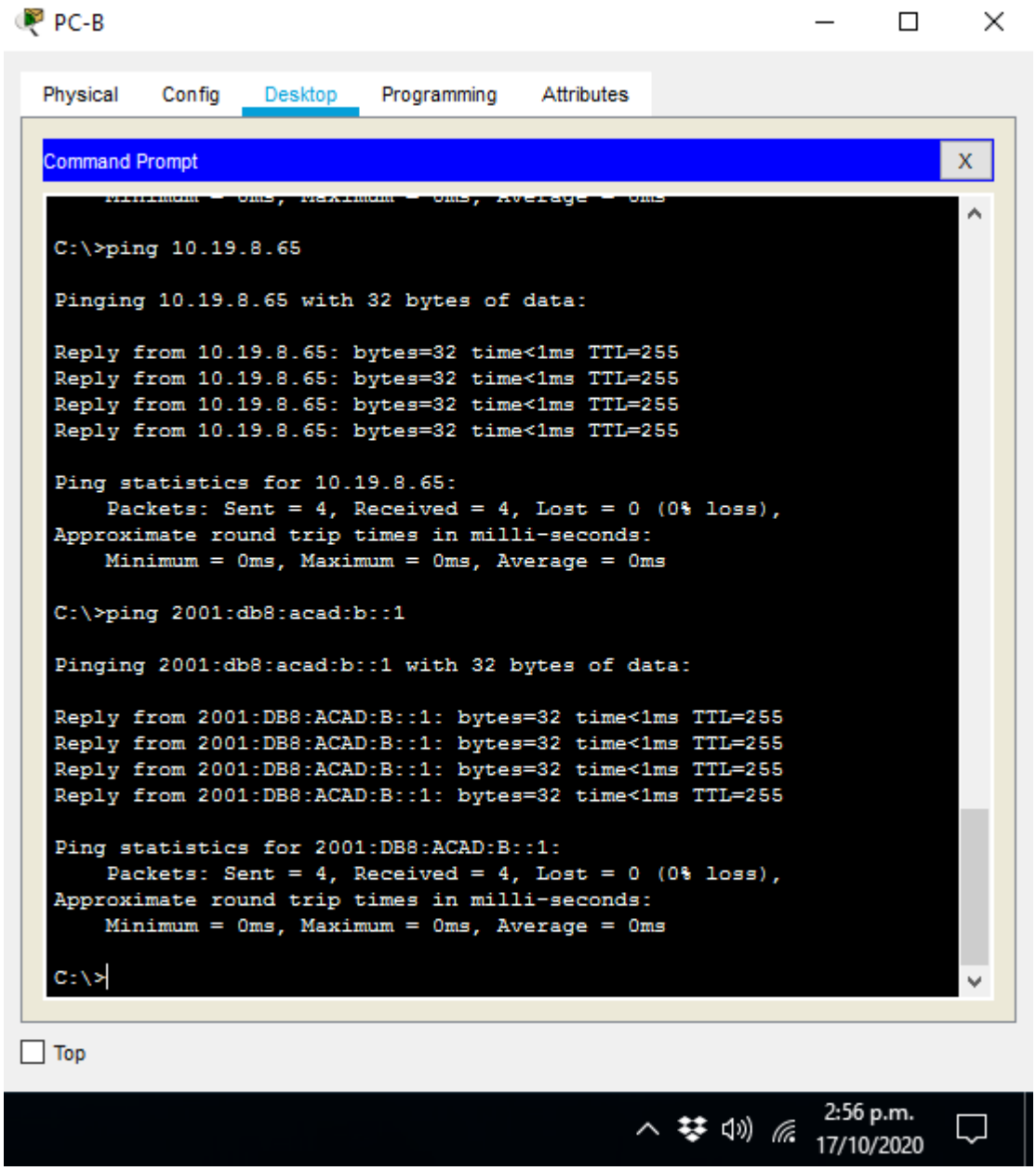


Figura 9. Ping de PC-B a R1 G0/0/1.3.

R1, G0/0/1.4

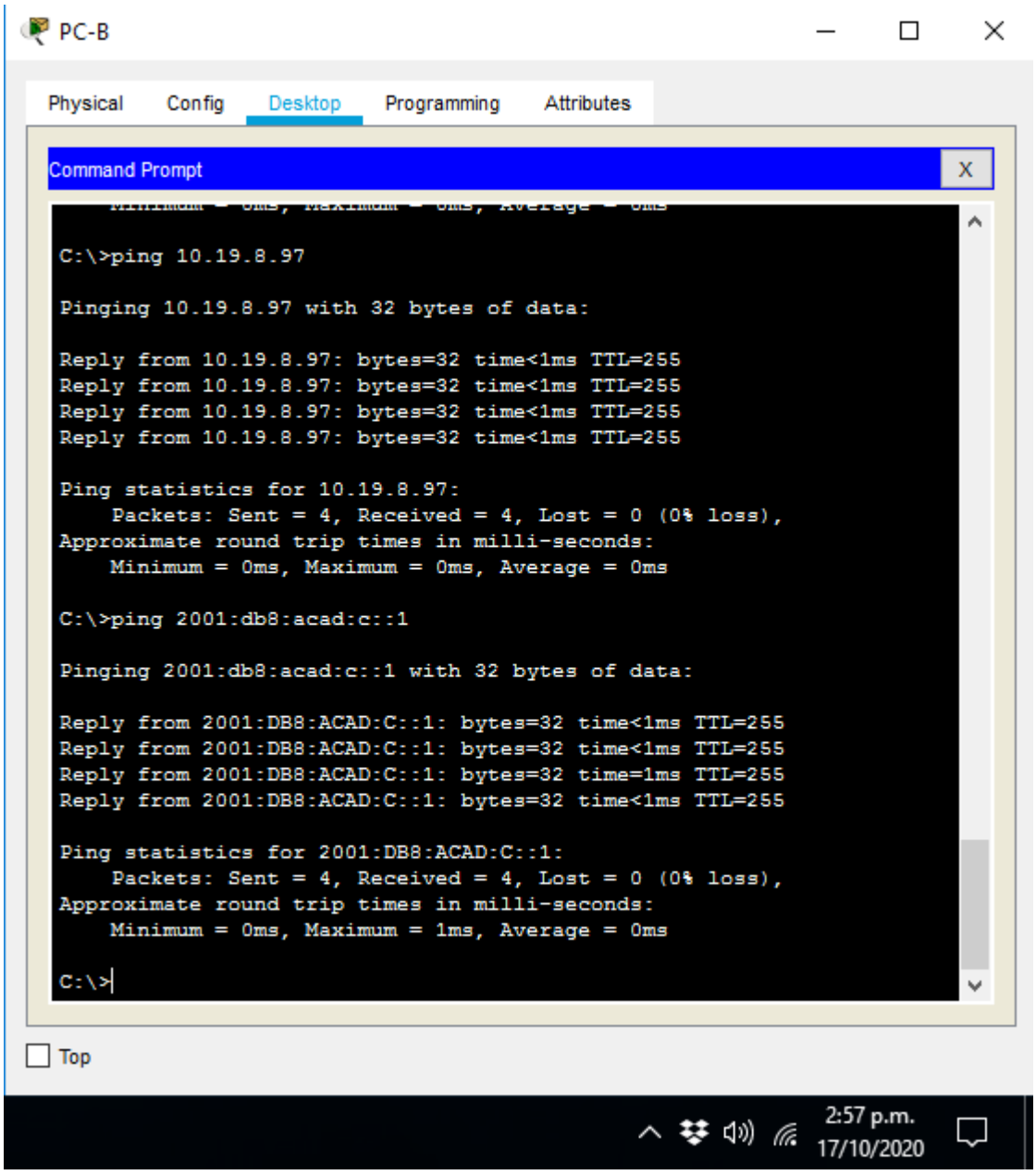


Figura 10. Ping de PC-B a R1 G0/0/1.4.

S1, VLAN 4

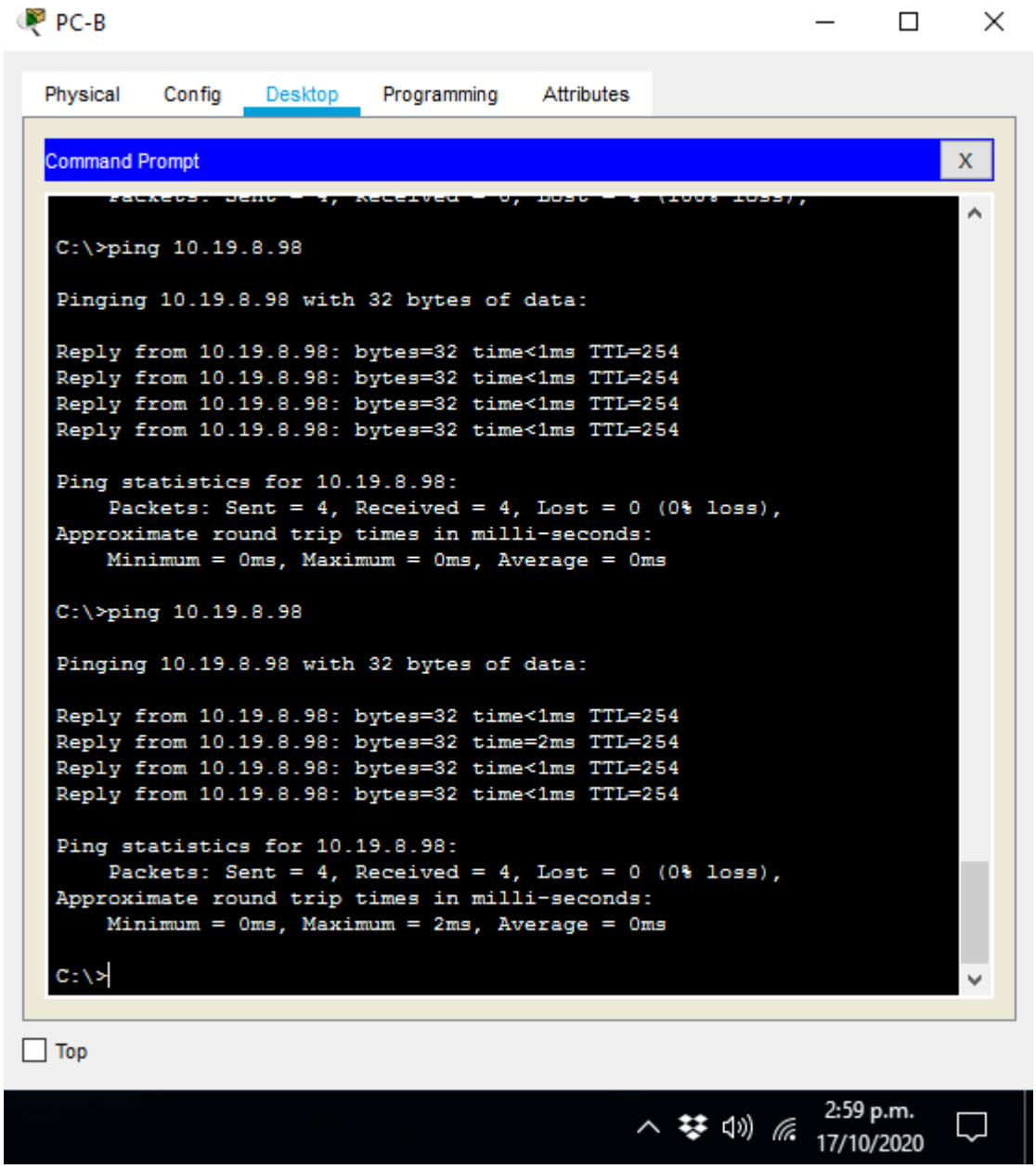


Figura 11. Ping de PC-B a S1 VLAN 4.

S2, VLAN 4

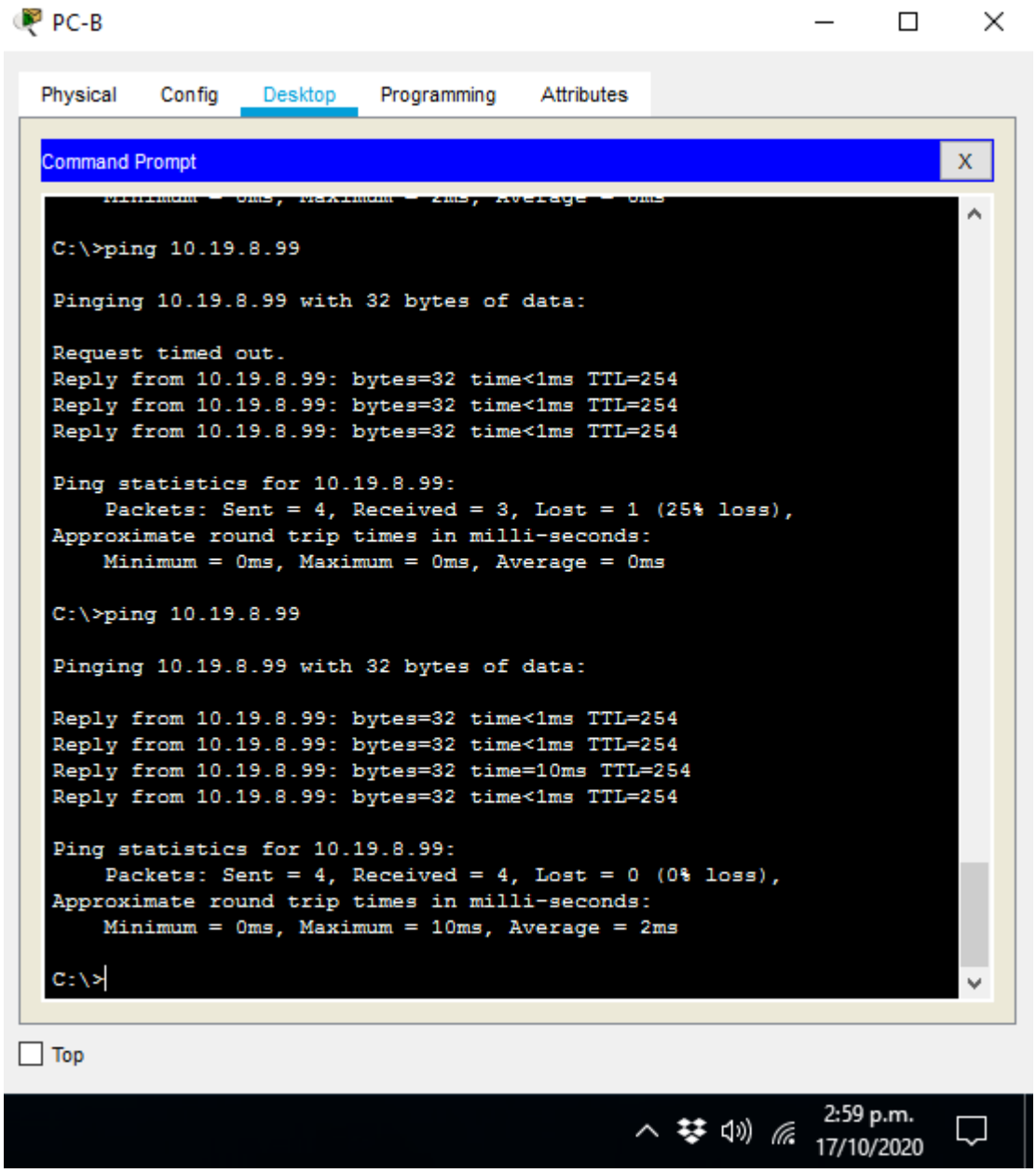


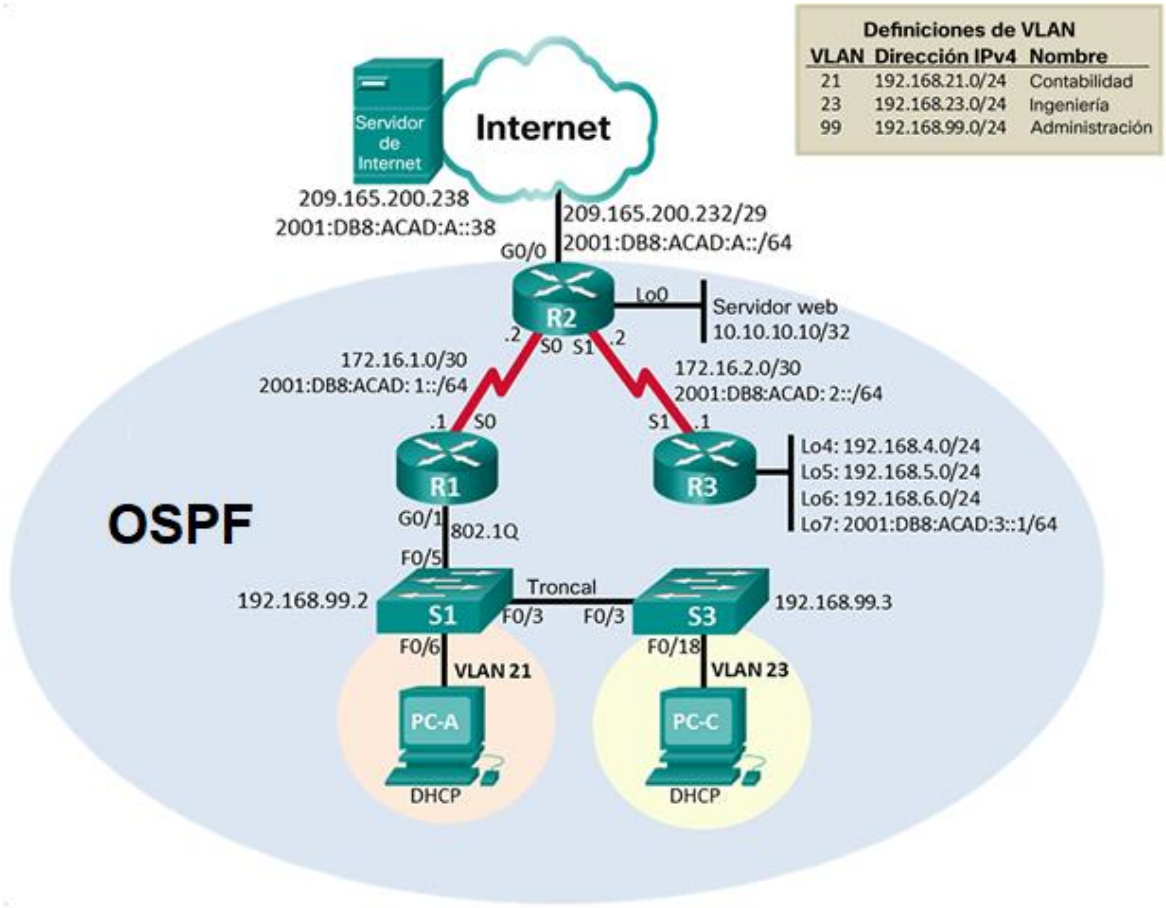
Figura 12. Ping de PC-B a S2 VLAN 4.

2.2. Escenario 2

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.

Topología.

Figura 13. Topología del escenario 2



Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

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

Tabla 12. Reinicio y verifcación de Router y Switches del escenario

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase sta Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch#

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

Tabla 13. Configuración de la computadora 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::2/64
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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración del Router R1

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

Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ipv6 unicas R1(config)#ipv6 unicast-routing R1(config)#

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 15. Configuración del Router R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit

Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit

Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 R2(config)#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 16. Configuración del Router R3

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

Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description R3 a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)# R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)# R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)# R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit.
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 17. Configuración del Switch S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohibe el acceso no autorizado#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 18. Configuración del Switch S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3

Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#

Paso 7: Verificar la conectividad de la red

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

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

Tabla 19. Verificación de la conectividad de los dispositivos

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:

			!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/10 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

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

Figura 14. Ping de R1 a R2.

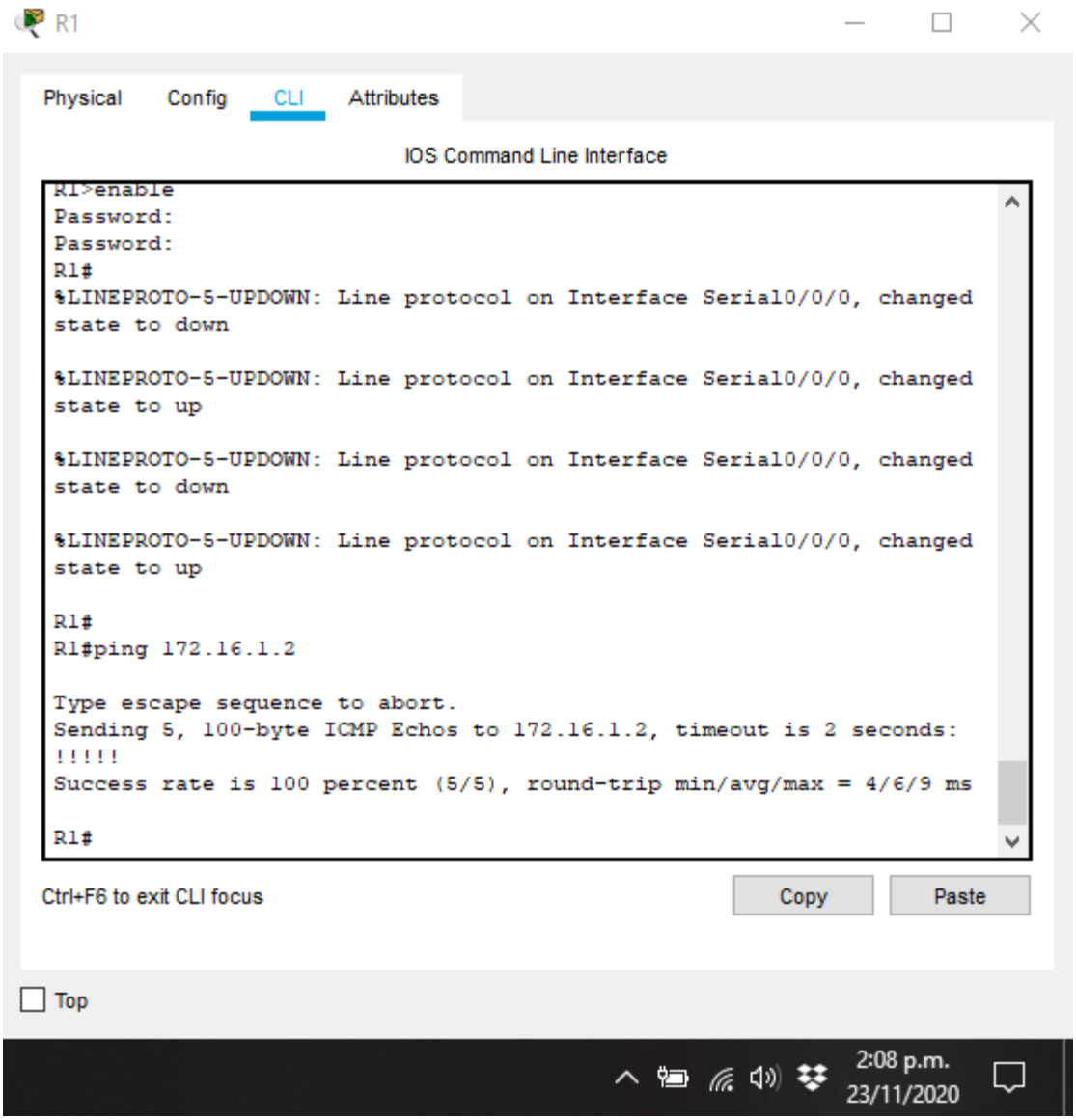


Figura 15. Ping de R2 a R3.

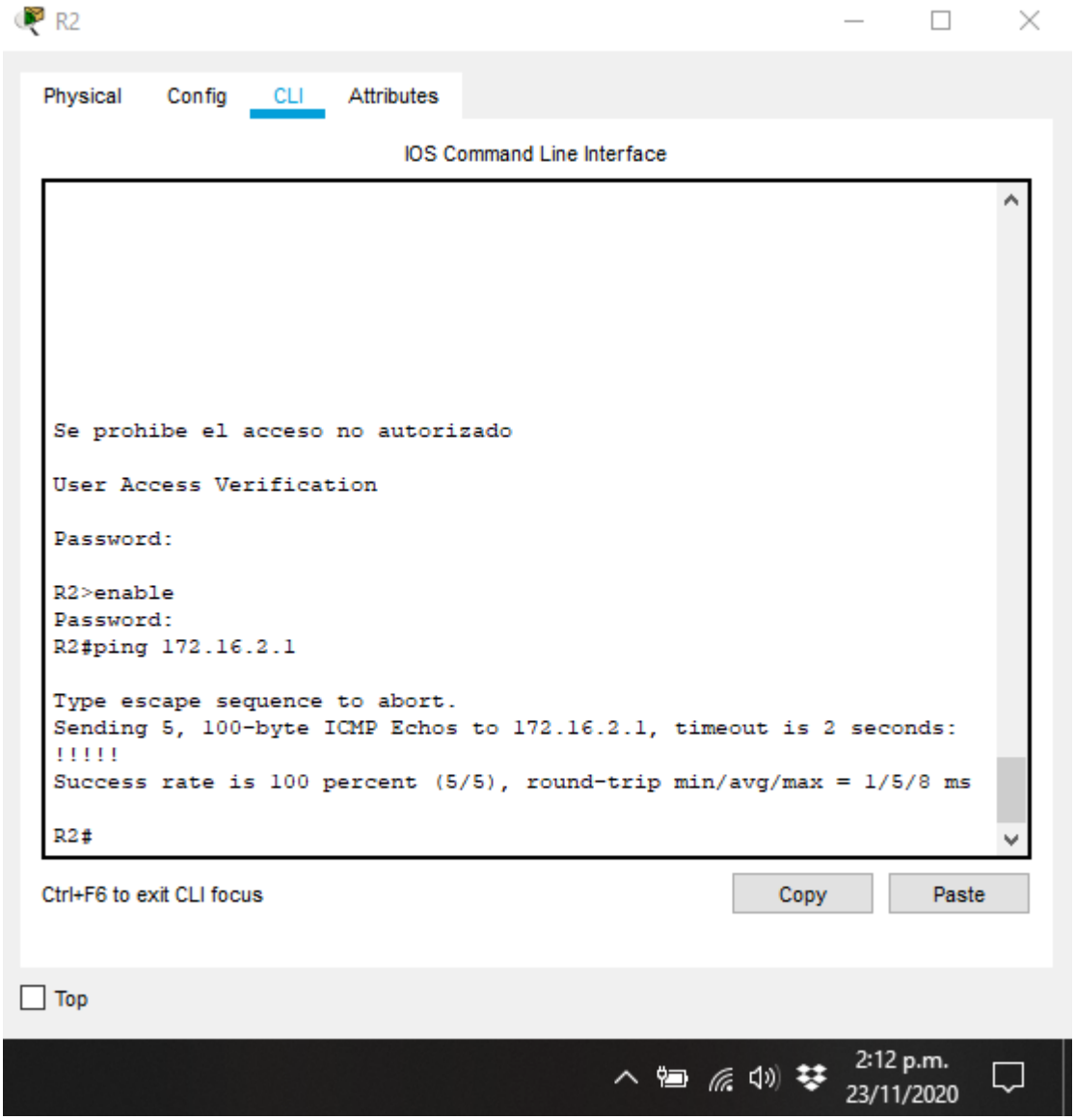
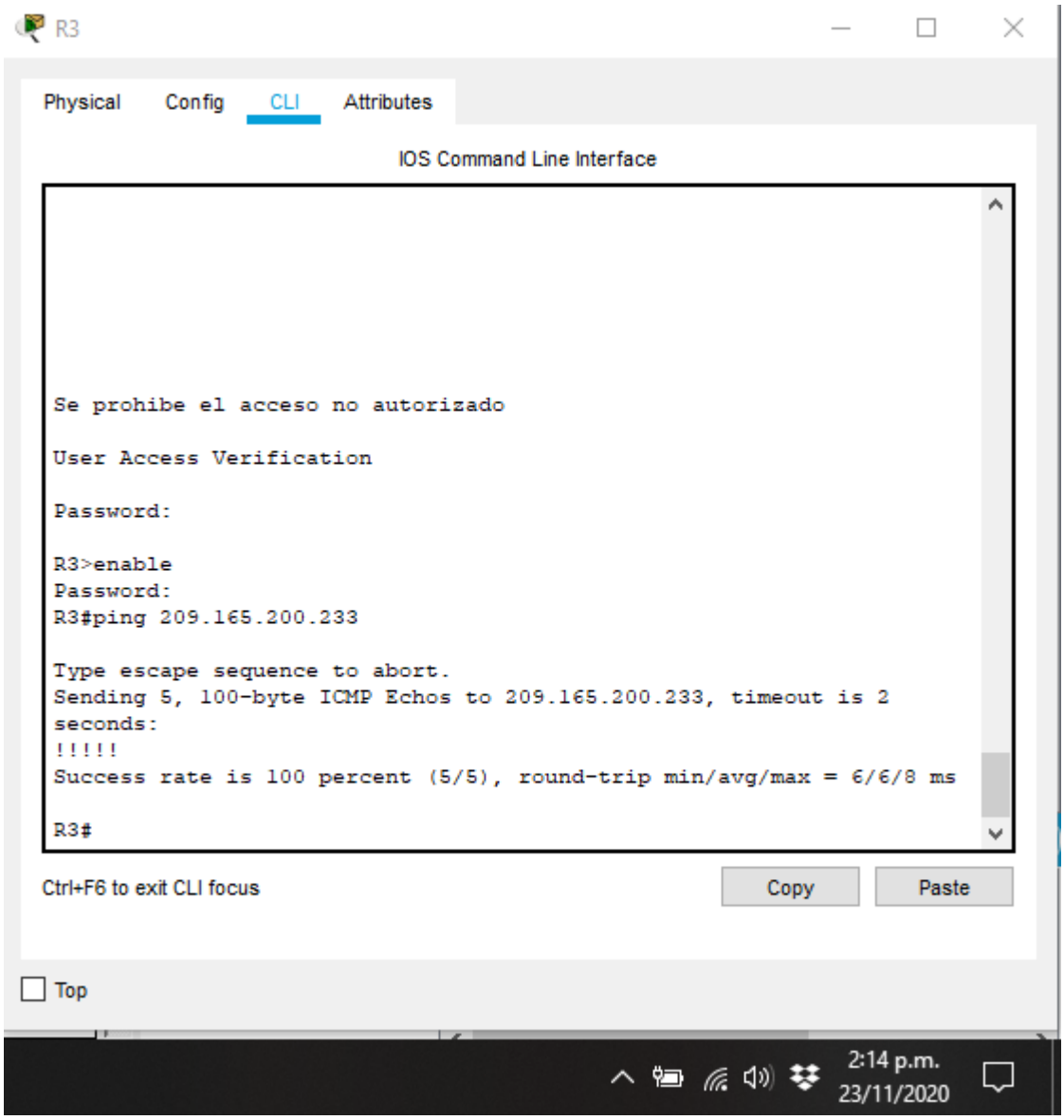


Figura 16. Ping de PC de Internet a Gateway predeterminado.



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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 20. Configuracion de la seguridad del Switch S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)# S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit

Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 21. Configuracion de la seguridad del Switch S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)# S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit

Asignar F0/18 a la VLAN 21	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuracion de la seguridad del Router R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description accounting LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description accounting LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit

Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#exit

Paso 4: Verificar la conectividad de la red

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

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

Tabla 23. Verificación de la conectividad entre switches y R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1,

			timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

			S3#

Figura 17. Ping S1 a VLAN Administracion.

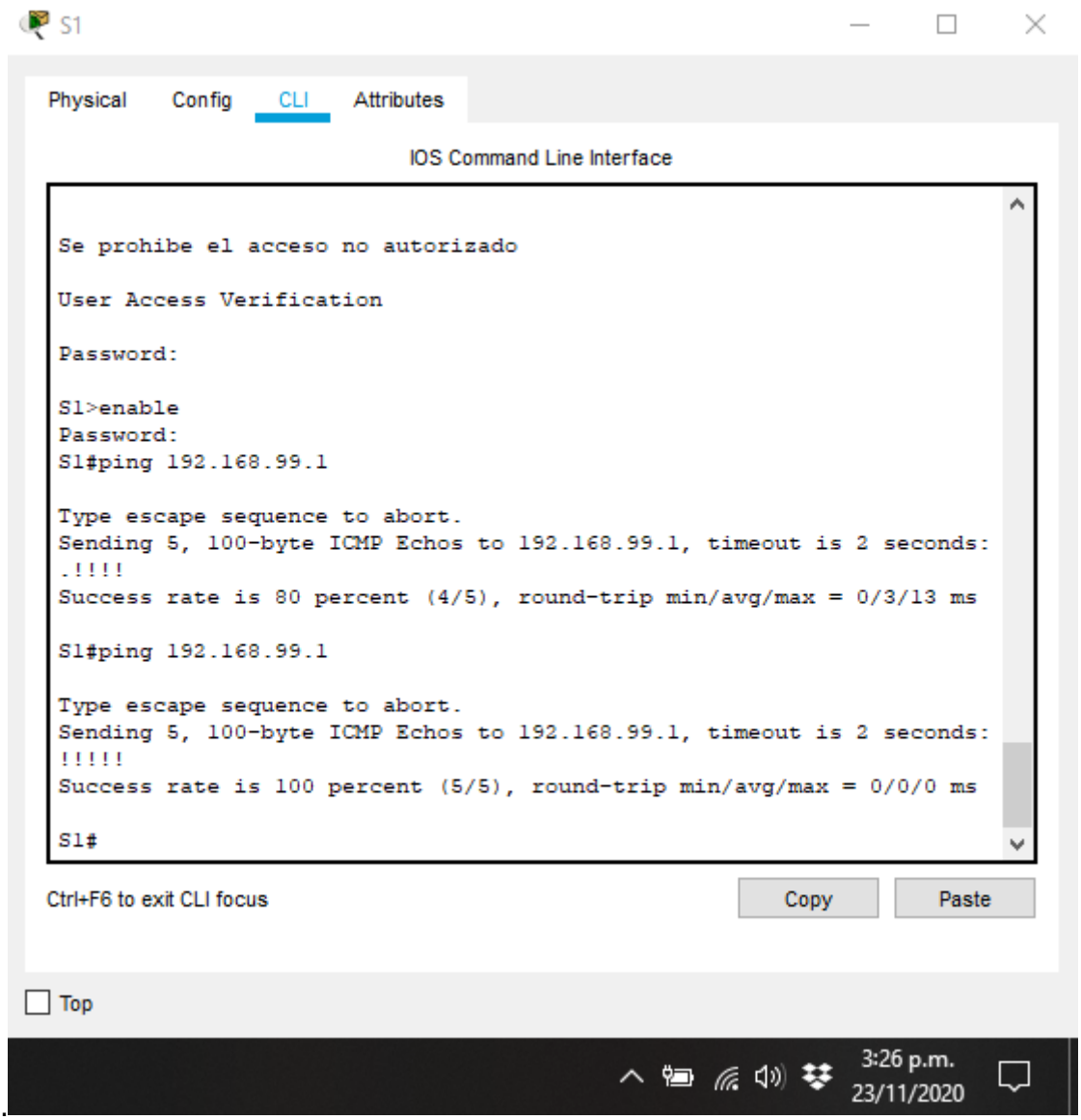


Figura 18. Ping S3 a VLAN Administracion.

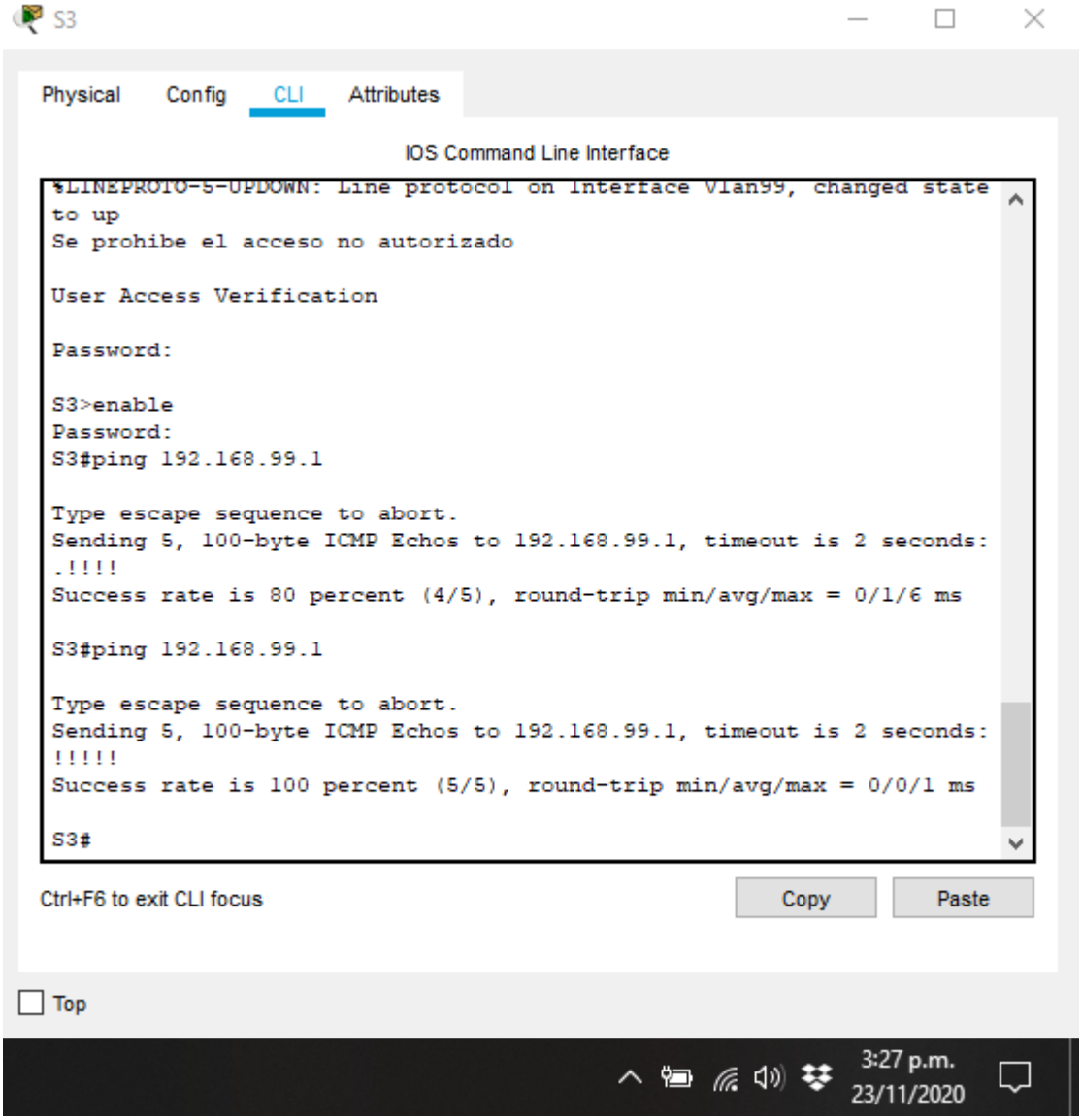


Figura 19. Ping de S1 a VLAN 21.

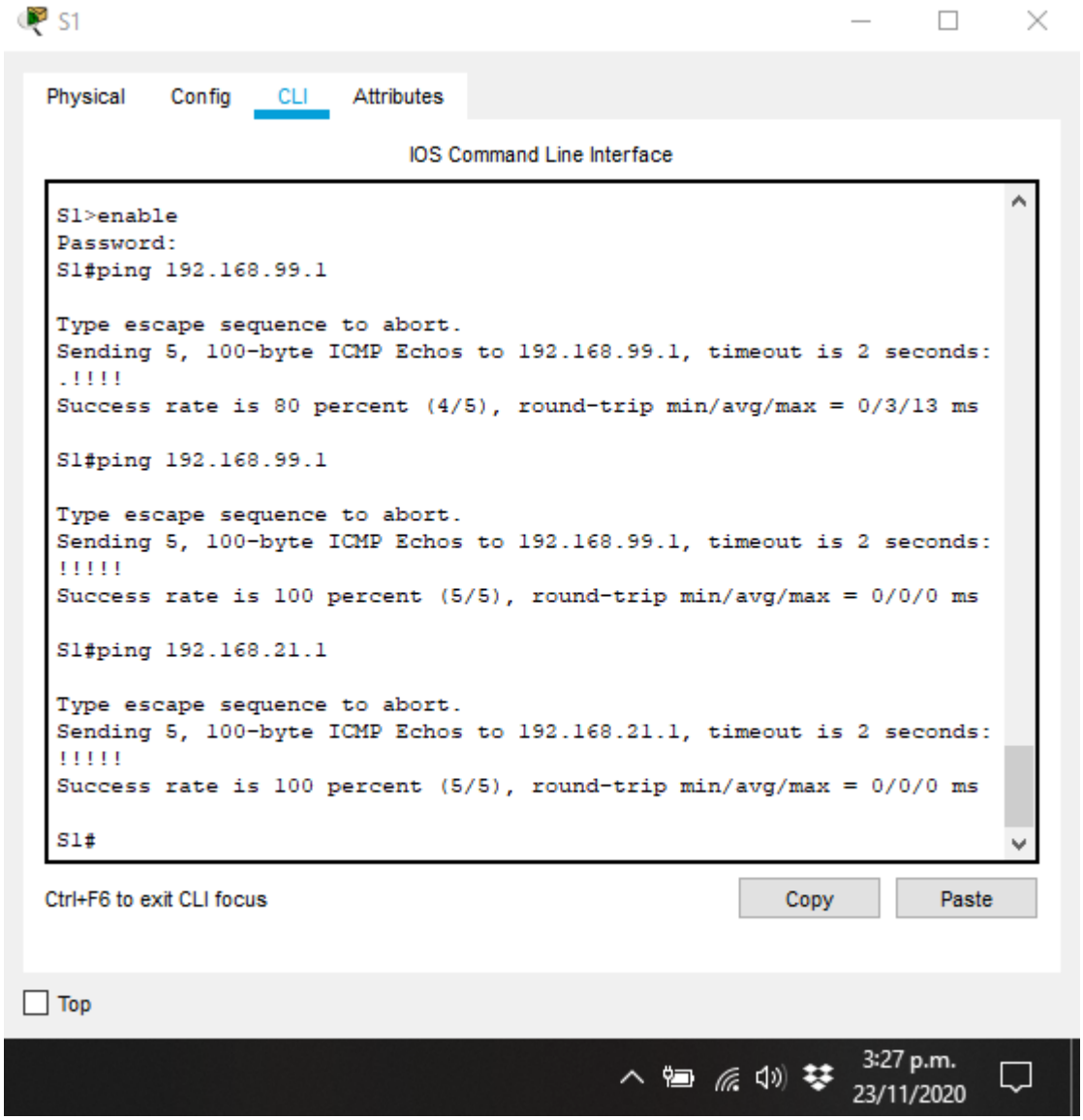
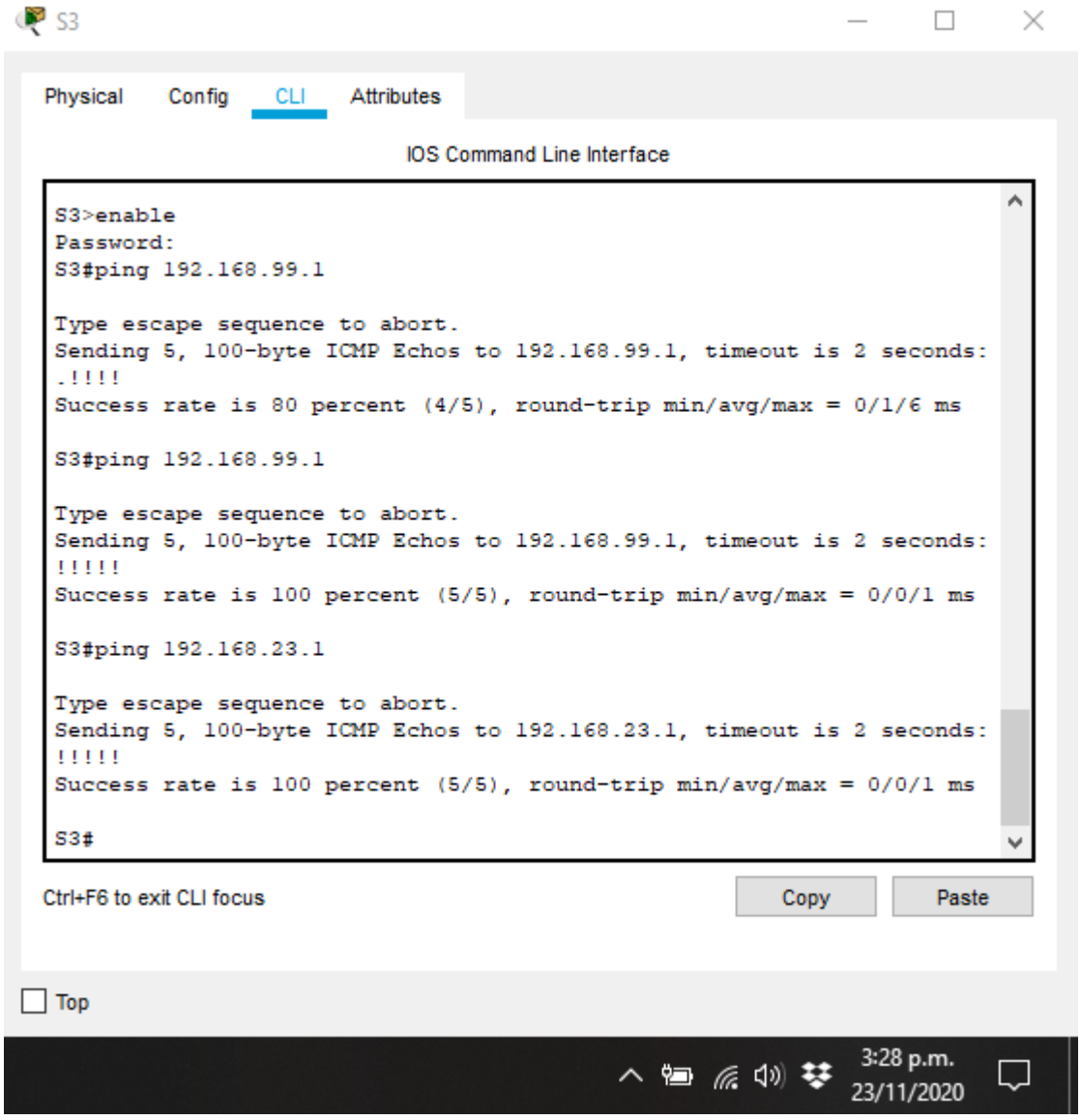


Figura 20. Ping de S3 a la VLAN 23.



Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuracion OSPF en el Router R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gi0/1.21 R1(config-router)#passive-interface gi0/1.23 R1(config-router)#passive-interface gi0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuracion OSPF en el Router R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1

Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 26. Configuracion OSPFv3 en el Router R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Paso 4: Verificar la información de OSPF

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

Tabla 27. Verificación información de 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 ip ospf database

Figura 21. Comando para ver ID del proceso OSPF.

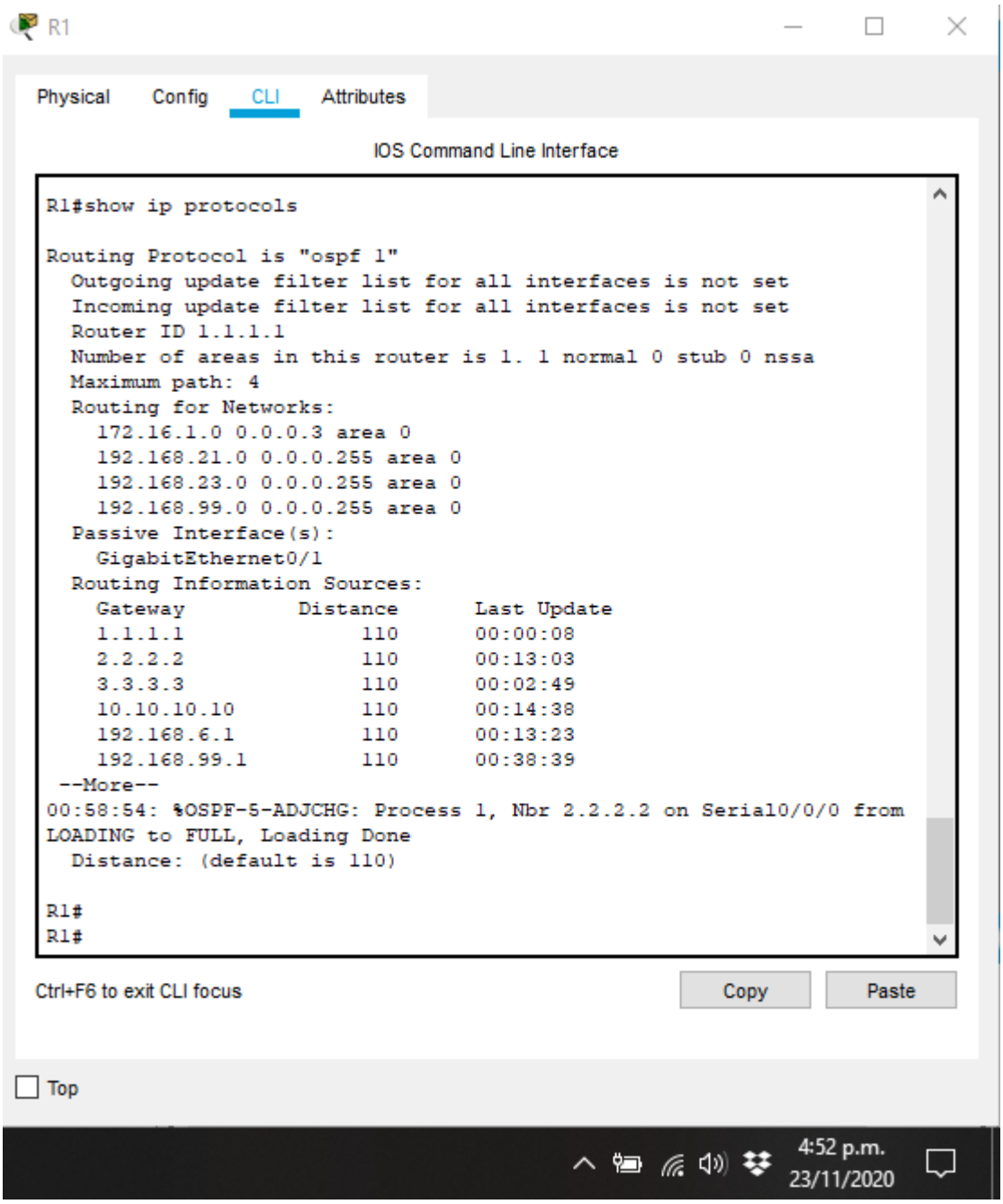


Figura 22. Comando para mostrar solo las rutas OSPF.

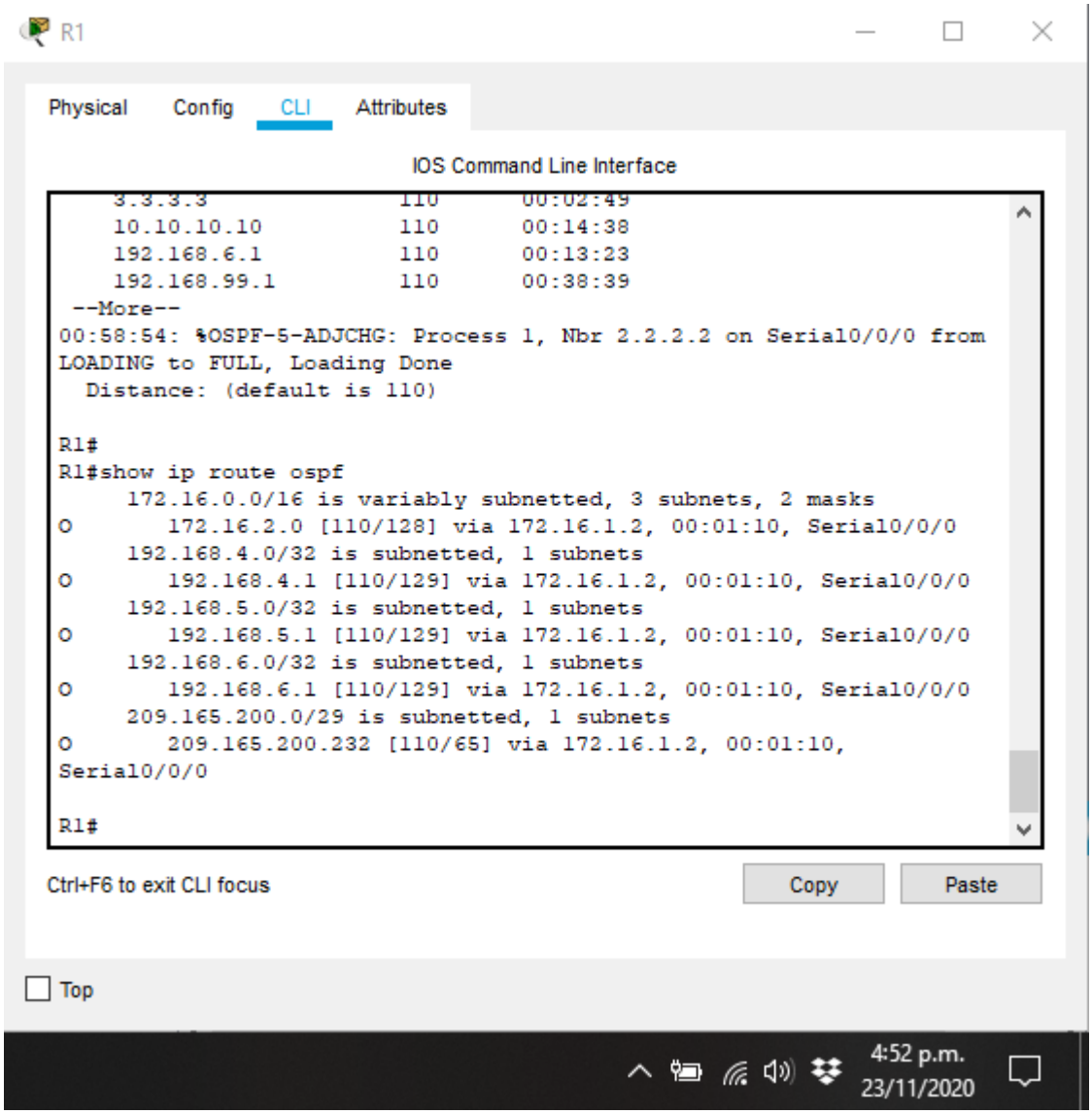
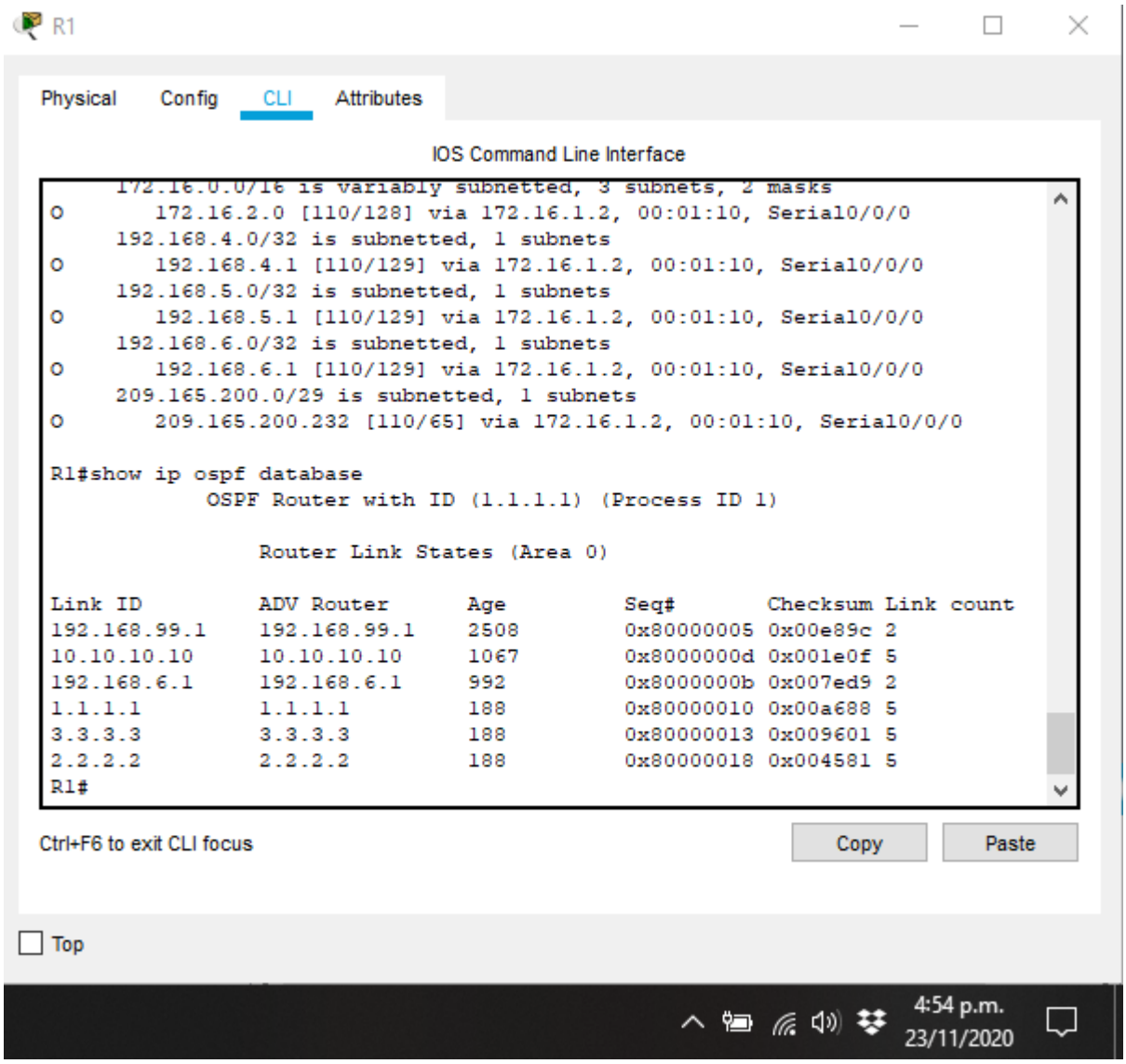


Figura 23. Muestra la sección de OSPF de la configuración en ejecución.



Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 28. Configuración R1 como servidor DHCP para VLAN 21 y 33

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

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

La configuración del R2 incluye las siguientes tareas:

Tabla 29. Configuración NAT estática y dinámica en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 30. Verificación del protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	

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**	

Figura 24. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

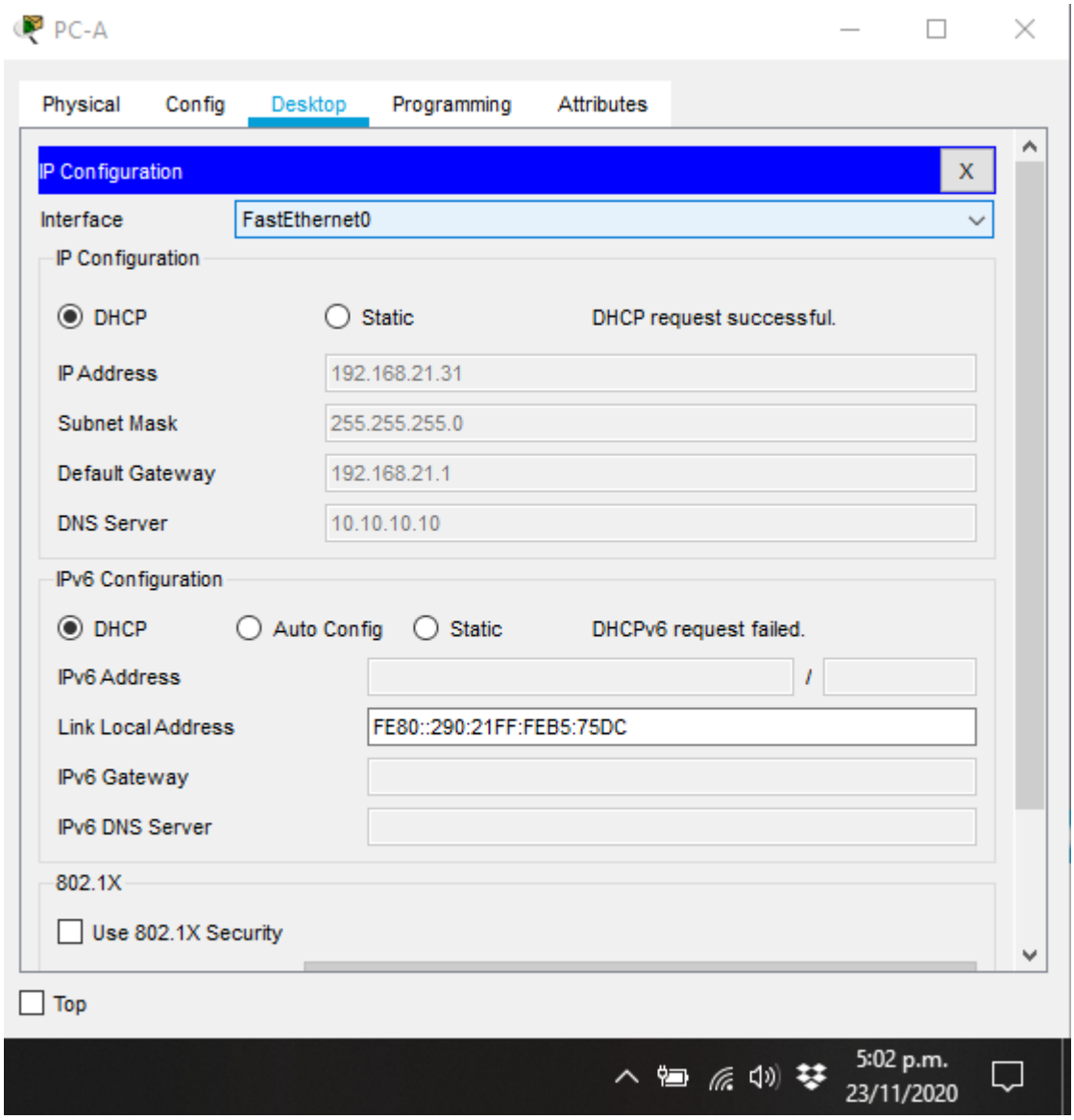


Figura 25. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

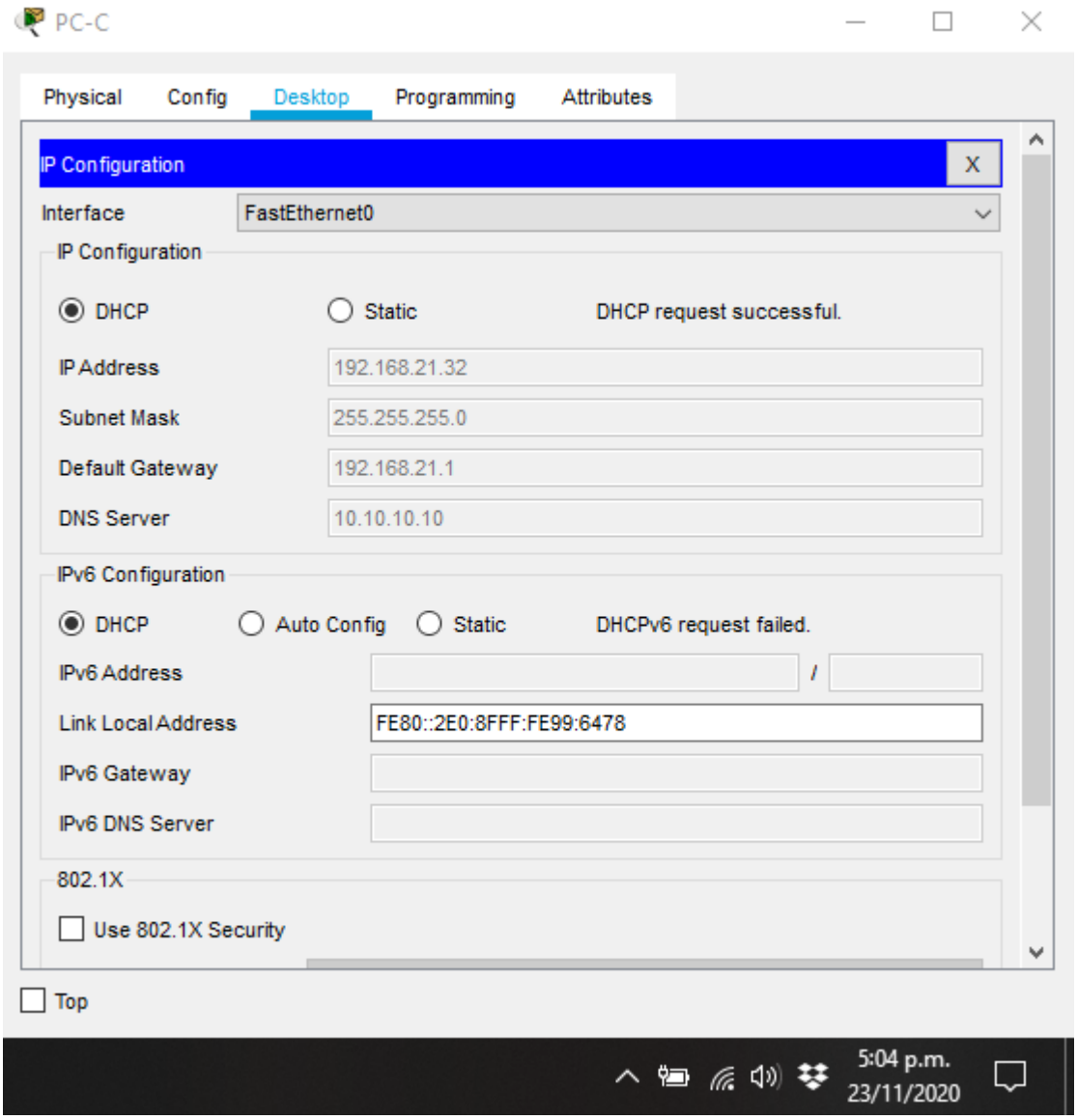


Figura 26. Verificar que la PC-A pueda hacer ping a la PC-C.

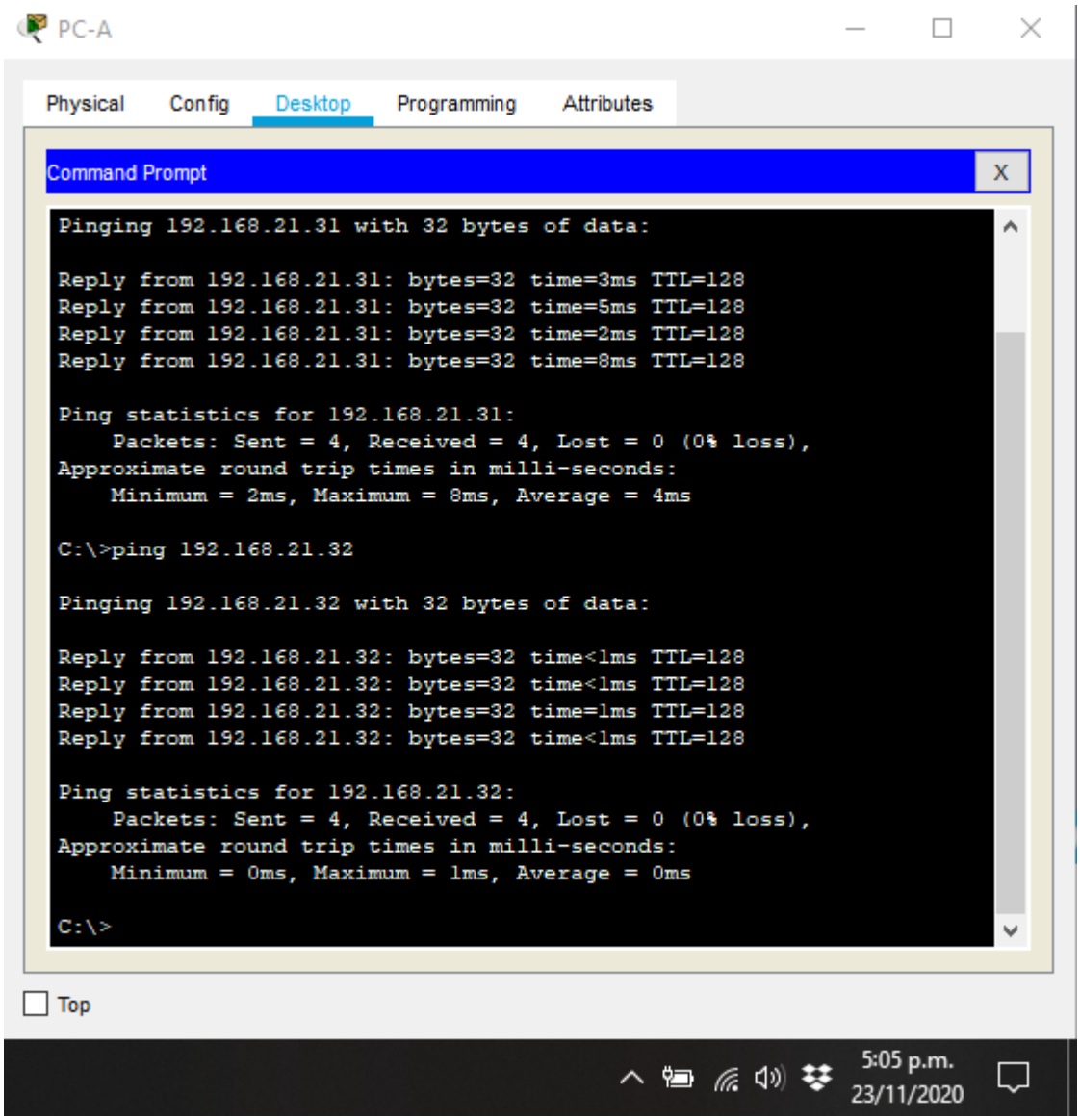
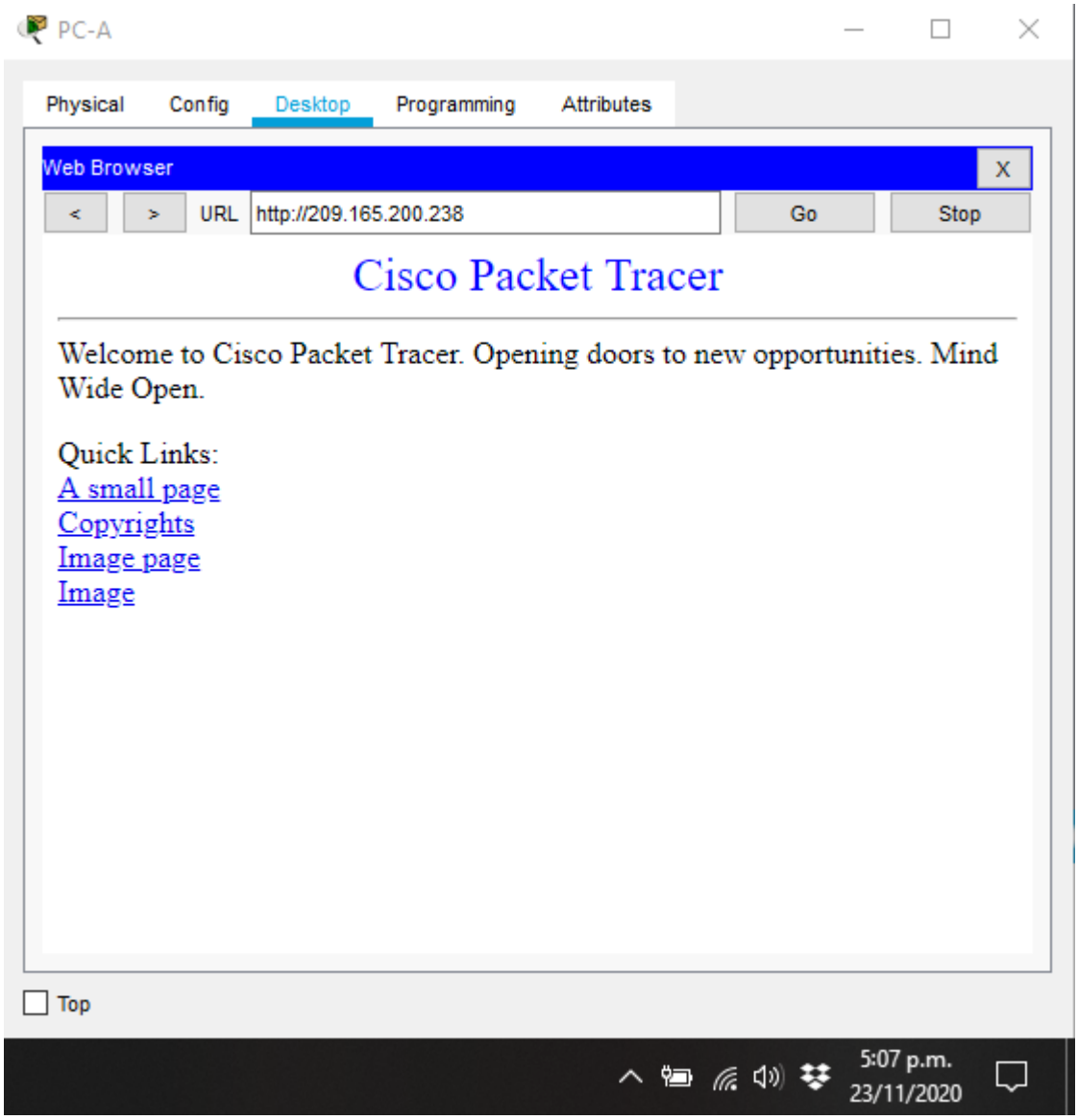


Figura 27. navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229).

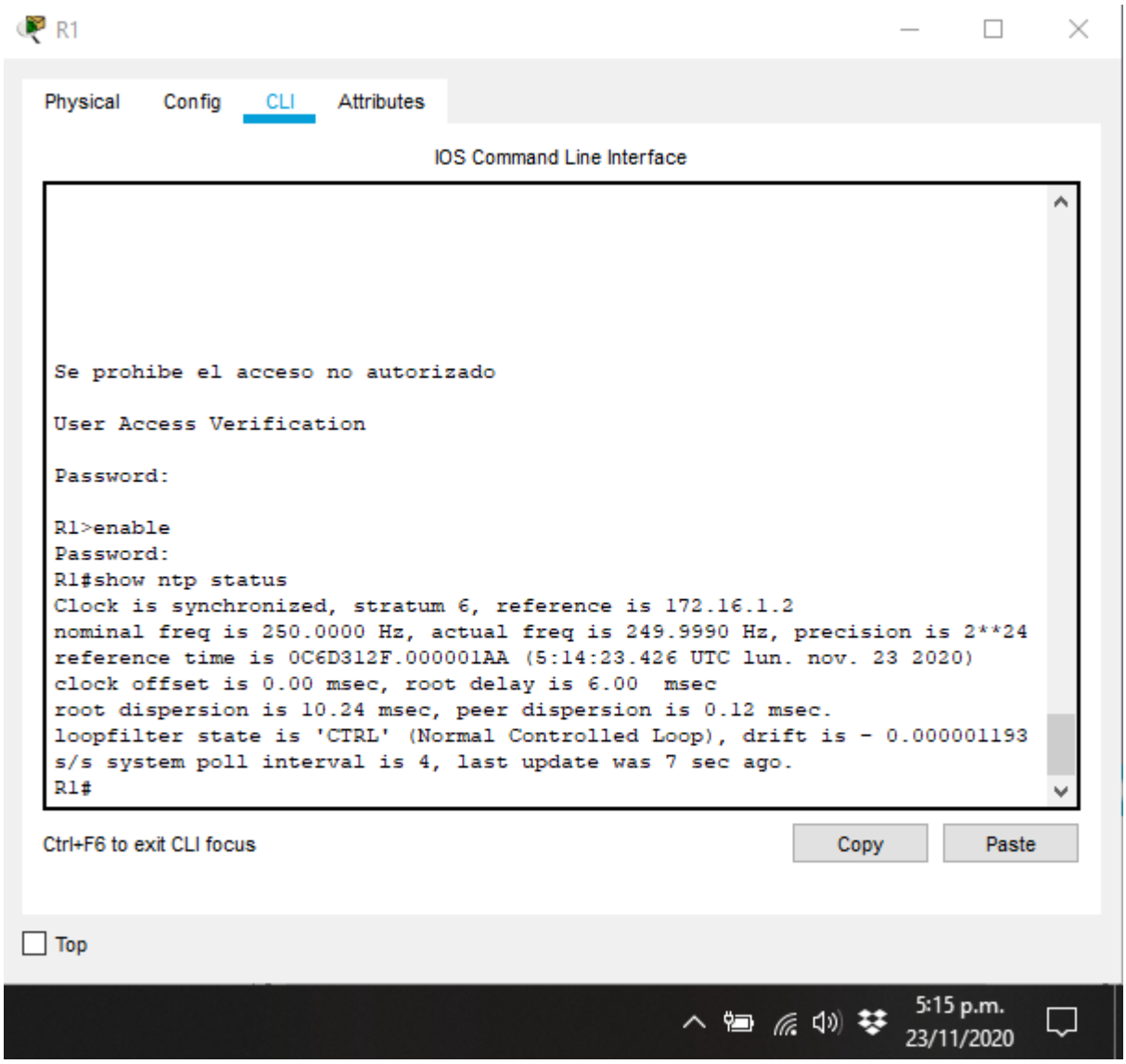


Parte 6: Configurar NTP

Tabla 31. Configuración NTP en R1

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 02:22:50 13 May 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	

Figura 28. Verifique la configuración de NTP en R1.



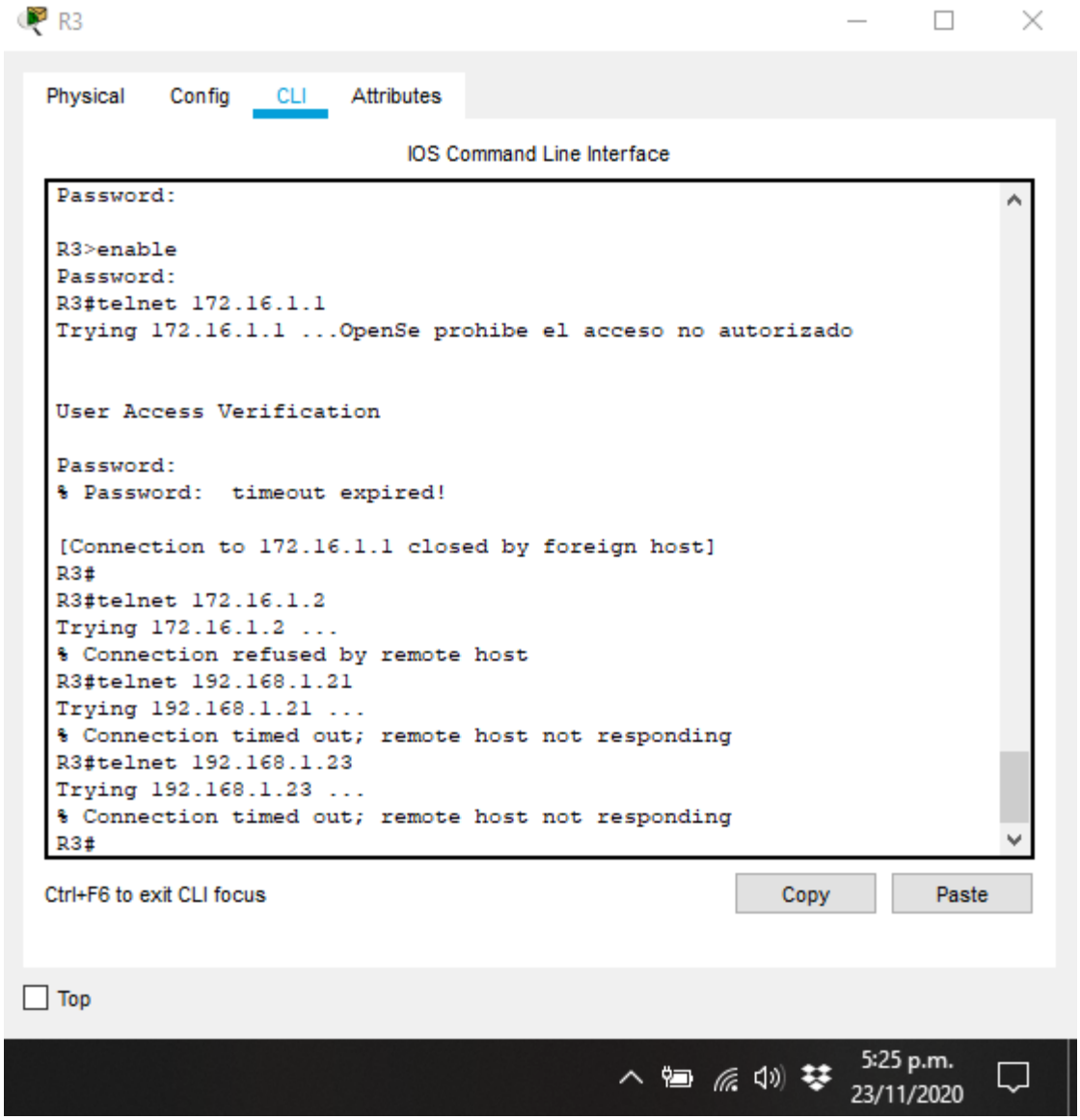
Parte 7. Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 32. Restringir el acceso a las lineas VTY en Router R2

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

Figura 29. Verificación del funcionamiento de la ACL.



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

Tabla 33. Comandos de verificación

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1(config)#show access-list
Restablecer los contadores de una lista de acceso	R1(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1 (config)#interface Fa0/1 R1 (config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	R1 (config)#show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

CONCLUSIONES

Con el desarrollo de esta prueba se comprende la mayoría de los conceptos vistos en el transcurso del curso del diplomado de profundización cisco y ayuda a desenvolverse teniendo como base estos escenarios que son asociados a problemas en la vida cotidiana

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

Se identifica las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches.

Finalmente, durante la evaluación, se probó y registró la red mediante los comandos comunes de CLI.

BIBLIOGRAFÍA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Anexo 1. Artículo científico IEEE

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Onofre Mejía Romero
omejiar@unadvirtual.edu.co
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Universidad Nacional Abierta y a Distancia (UNAD)

Resumen

La evaluación denominada "Prueba de habilidades prácticas", forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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.

Para el segundo escenario, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente.

Palabras Clave: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

Abstract - The evaluation called "Test of practical skills" is part of the evaluative activities of the CCNA Deepening Diploma, and seeks to identify the degree of development of skills and abilities that were acquired throughout the diploma. The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking.

In this first scenario, the devices of a small network will be configured. You must configure a router, switch, and computers that support both IPv4 and IPv6 connectivity for the supported hosts. The router and switch must also be managed securely. You will configure routing between VLAN, DHCP, Etherchannel, and port-security.

For the second scenario, a small network must be configured to support IPv4 and IPv6 connectivity, switch security, inter-VLAN routing, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), address translation dynamic and static network (NAT), access control lists (ACLs), and network time protocol (NTP) server / client.

Keywords: CISCO, Switching, Routing, Networks, Systems

INTRODUCCIÓN

Para esta actividad, se dispone de un tiempo para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de

las siguientes herramientas: Packet Tracer o GNS3.

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. Para el segundo escenario, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, y demás configuraciones que contribuyen a la correcta solución del escenario.

Al final, cada proceso está debidamente documentado y consta de una evidencia que determina la operación y aplicación de cada una de las instrucciones requeridas para el cumplimiento de lo solicitado en cada uno de los escenarios y además de verificar el funcionamiento y el comportamiento de la red a medida que se va implementando cada uno de los cambios y configuración de los dispositivos.

I. PROCEDIMIENTO PARA ADMINISTRAR UNA RED LAN USANDO OSPF

El procedimiento para llevar a cabo la configuración del protocolo OSPF (Open Shortest Path First) de la siguiente pequeña red, se realiza por medio de los siguientes pasos y estos son:

Topología de la red

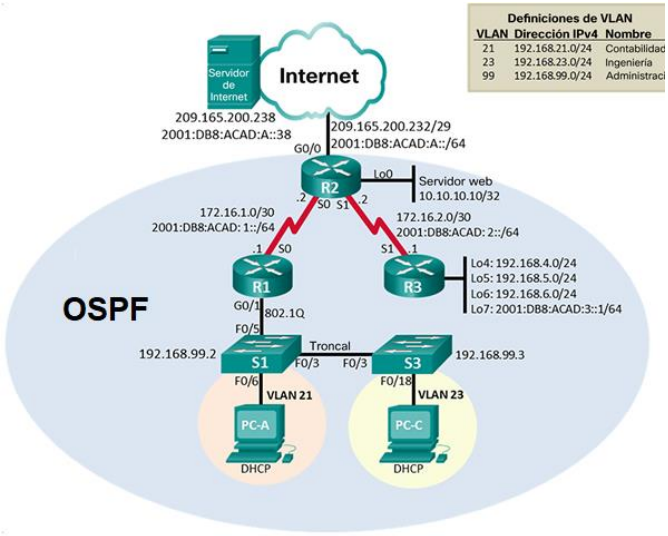


Figura 1. Topología de la red

Para realizar la topología de la red, tal como se muestra en la Figura 1, inicialmente agregamos a la pantalla principal del programa tres router 2901 y se conectan los dispositivos por los puertos serial s0/3/0 y s0/3/1, como podemos observar en la topología de la red, seguidamente se agregan los switch y se realizan las conexiones por medio de puertos seriales al router y al host según corresponda.

Inicialización de los dispositivos

Hay que asegurarnos que los routers no tengan configuraciones previas, entonces por medio del comando erase startup-config eliminamos toda configuración y con el comando reload se volverán a cargar los dispositivos.

TABLA 1
VERIFICACION INICIAL DE LOS DISPOSITIVOS

•

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

En la tabla I se muestran los comandos. Para realizar las configuraciones de formateo y reinicio tanto en los Routers como en los Switch.

Configuración de los parámetros básicos en los dispositivos

Las tareas de configuración del servidor de Internet incluyen lo siguiente.

TABLA 2
VERIFICACION INICIAL DE LOS DISPOSITIVOS EN EL ROUTER 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class

Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ipv6 unicas R1(config)#ipv6 unicast-routing R1(config)#

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.

Las tareas de configuración para R1, R2 y R3 incluyen las siguientes:

TABLA 3
VERIFICACION INICIAL DE LOS DISPOSITIVOS EN EL ROUTER 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit

Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 R2(config)#

Después de realizar las configuraciones básicas en los dispositivos es importante por medio del comando ping probar la conectividad entre los dispositivos de red.

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

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1.
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)# S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Una vez realizada la creación y configuración de las VLAN en S1 y S3, procedemos a configurar la interfaz G0/1. Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description accounting LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description accounting LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit

Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown R1(config-if)#exit

CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

En esta sección se describen los comandos para realizar la configuración OSPF en la red. Las tareas de configuración para R1 son:

Configurar OSPF área 0

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gi0/1.21 R1(config-router)#passive-interface gi0/1.23 R1(config-router)#passive-interface gi0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

VERIFICAR LA INFORMACIÓN DE OSPF

Después de realizar las configuraciones anteriores en los dispositivos verificamos que OSPF esté funcionando como se espera. Por medio de los siguientes comandos.

TABLA 2
COMANDOS PARA RELIZAR LAS VERIFICACIONES DE LAS CONFIGURACIONES DEL PROTOCOLO OSPF

Descripcion	**Comando**
Muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router	R1#Show ip protocols R2#Show ip protocols R3#Show ip protocols
Muestra solo las rutas OSPF	R1#Show ip route ospf R2#Show ip route ospf R3#Show ip route ospf
Muestra la sección de OSPF de la configuración en ejecución	R1#Show run R2#Show run R3#Show run

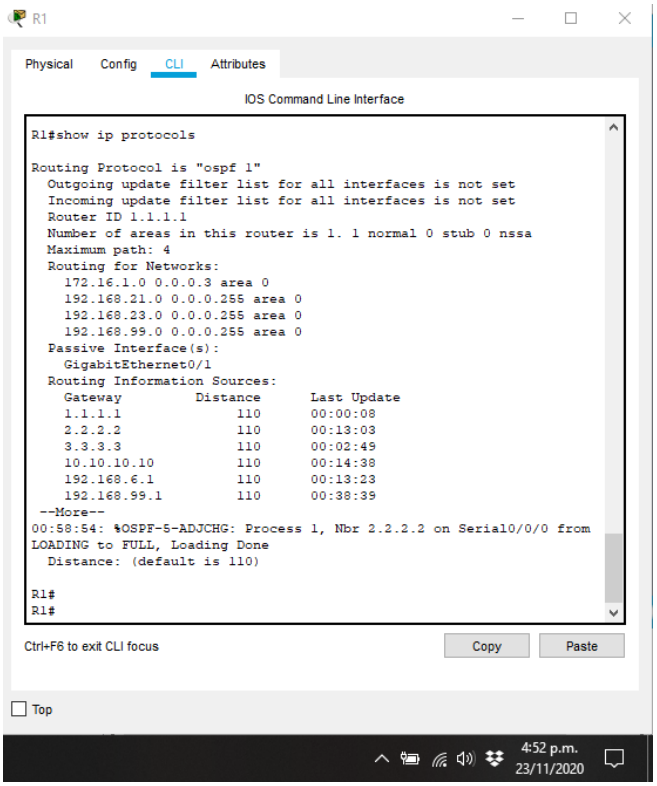


Figura 1. Comando para ver ID del proceso OSPF

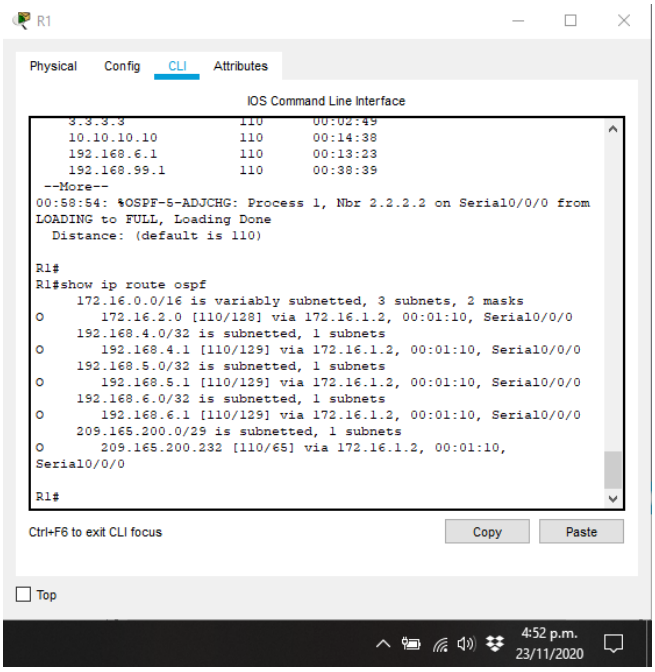


Figura 2. Comando para mostrar solo las rutas OSPF.

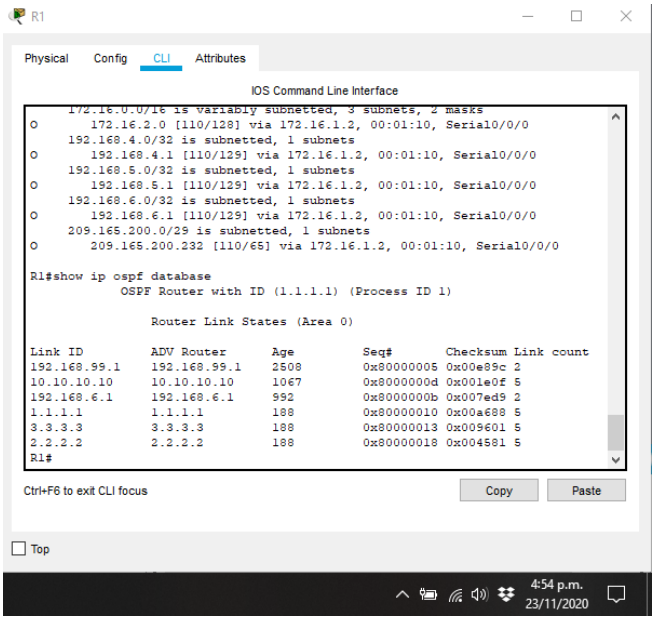


Figura 3. Muestra la sección de OSPF de la configuración en ejecución.

RESULTADOS

Las configuraciones realizadas permitieron observar que el protocolo OSPF, no es tan complejo de implementar porque su configuración es parecida a otros protocolos menos robustos y que permite gestionar redes grandes de una forma segura.

Realizar esta configuración pro medio del software cisco packet tracer permite que nos hagamos competentes en el campo profesional, debido a que este software nos acerca a cómo funciona una red real.

REFERENCIAS

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-

assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1
CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1
CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1
CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1
CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1
CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3