DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

EDWIN ALEXANDER BATANERO SOTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ-CUNDINAMARCA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

EDWIN ALEXANDER BATANERO SOTO

Diplomado de opción de grado presentado para optar el título de INGENIERO ELECTRÓNICO

DIRECTOR:
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ-CUNDINAMARCA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá Cundinamarca, 29 de noviembre de 2020

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CCNA: (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente, sobre infraestructuras de red e Internet. Está orientada a los profesionales que operan equipamiento de networking.

TRACEROUTE: Traceroute ytracert son comandos de diagnóstico de redes para mostrar las posibles rutas o caminos de los paquetes y medir las latencias de tránsito y los tiempos de ida y vuelta a través de redes de Protocolo de Internet. Permite seguir la pista de los paquetes que vienen desde un punto de red
IPv6: El IPv6 es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones

DHCP: El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP

ETHERCHANNEL: Es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet.

VLAN: Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física

RESÚMEN

El presente documento tiene como objetivo mostrar el paso a paso del desarrollo de dos escenarios planteados, la actividad denominada “DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNA”, lo conforma dos módulos CCNA1 y CCNA2, comprende temas de redes de conmutación, las configuraciones exigidas se realizan mediante el uso de VLAN, DHCP, ETHERCHANNEL, PORT-SECURITY, OSPF, NAT, ACL, NTP, el proyecto se usa como opción de grado para calificar para el grado de Ingeniería Electrónica, para el desarrollo de la actividad se hace uso del simulador exclusivo de Cisco Systems, Packet Tracer.

Palabras clave CISCO, CCNP, Conmutación, enrutamiento, Redes, Electrónica

ABSTRACT

The objective of this document is to show the step-by-step development of two proposed scenarios, the activity called "CISCO DEEPENING DIPLOMA TEST OF PRACTICAL SKILLS CCNA", it is made up of two modules CCNA1 and CCNA2, it includes topics of switching networks, configurations required are carried out through the use of VLAN, DHCP, ETHERCHANNEL, PORT-SECURITY, OSPF, NAT, ACL, NTP, the project is used as a degree option to qualify for the degree of Electronic Engineering, for the development of the activity it is done use of Cisco Systems exclusive simulator, Packet Tracer.

Keywords CISCO, CCNP, Switching, routing, Networks, Electronics

INTRODUCCIÓN

La implementación de la prueba de habilidades Cisco denominada “DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNA”, busca poner en práctica el conocimiento obtenido mediante el desarrollo de dos escenarios de redes de conmutación aplicando a groso modo el uso de los principales protocolos de enrutamiento, esta tecnología busca brindar soluciones de tecnología comunicativas, administrativas, de control y lo más importante de seguridad de la información donde se benefician personas del común y empresas

El primer escenario consta de una topología pequeña conformada por 5 equipos, se plantea la configuración de los router, switch y demás equipo buscando que se admita la conectividad de dichos equipos con la conectividad IPv4 como IPv6, los equipos se deben configurar de tal forma que permitan la administración de forma segura, la configuración del enrutamiento se efectuará entre VLAN, DHCP, Etherchannel y port-security.

En el segundo escenario se debe configurar una red pequeña 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 se prueba y se registra la red mediante los comandos comunes de CLI.

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1. ESCENARIO 1

Descripción general

Registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

El estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

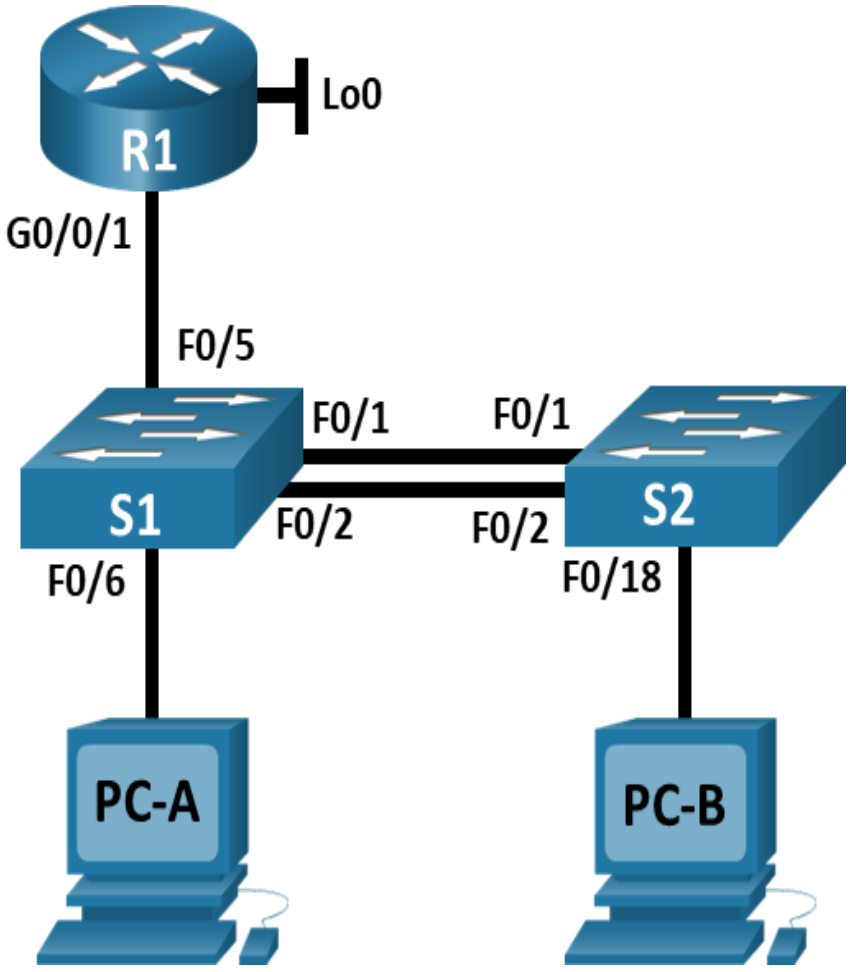


Figura 1. Topología1

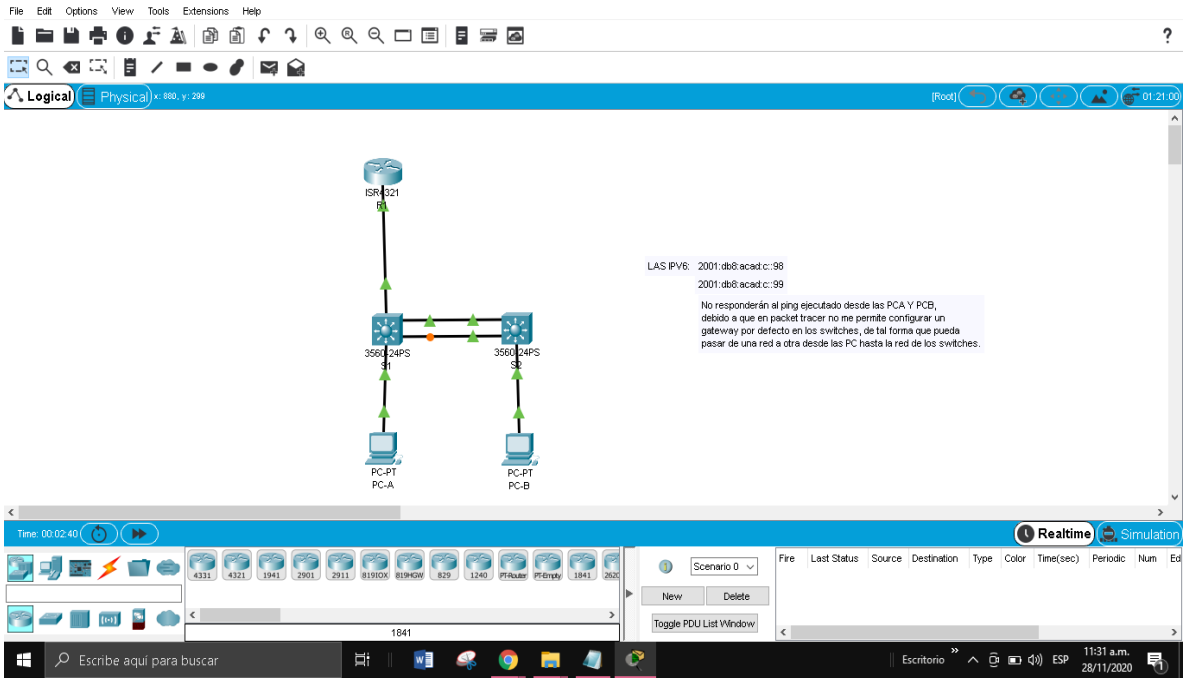


Figura 2. Topología 1 montada en simulador Packet Tracer

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 de VLAN

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

Tabla 1. Tabla de VLAN

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
		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
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Tabla 2.Tabla de asignación de direcciones

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

Instrucciones:

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.

Para ejecutar lo solicitado se realiza el siguiente procedimiento en la totalidad router y switches de la topología propuesta.

Enable

Erase startup-config

Delete flash:vlans.dat

Reload.

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

Esto no es posible en packet tracer debido a que solo se puede aplicar al modo real de los equipos.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

En la siguiente tabla podemos observar la configuración realizada para cumplir con lo solicitado en el presente ítem.

Tarea	Especificación
Desactivar la búsqueda DNS	enable configure terminal No ip domain lookup
Nombre del router	Enable Configure terminal Hostname R1

Tarea	Especificación
Nombre de dominio	Enable Configure terminal Ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Enable Configure terminal Enable secret ciscoenpass
Contraseña de acceso a la consola	Enable Configure terminal Line console 0 Password ciscoconpass Login
Establecer la longitud mínima para las contraseñas	Enable Configure terminal security password min-length 10 caracteres
Crear un usuario administrativo en la base de datos local admin con password admin1pass	Enable Configure terminal Username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Enable Configure terminal Line vty 0 15 Login local
Configurar VTY solo aceptando SSH	Enable Configure terminal Line vty 0 15 Transport input ssh
Cifrar las contraseñas de texto no cifrado	Servie password-encryption
Configure un MOTD Banner	Banner motd & Bienvenido &
Habilitar el routing IPv6	Enable Configure terminal Ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	Enable Configure terminal interface GigabitEthernet0/0/1 ipv6 address FE80::1 link-local ipv6 enable no shutdown interface GigabitEthernet0/0/1.2 encapsulation dot1Q 2 ip address 10.19.8.1 255.255.255.192 ipv6 address 2001:DB8:ACAD:A::1/64 ipv6 enable interface GigabitEthernet0/0/1.3 encapsulation dot1Q 3 ip address 10.19.8.65 255.255.255.224 ipv6 address 2001:DB8:ACAD:B::1/64 ipv6 enable interface GigabitEthernet0/0/1.4 encapsulation dot1Q 4 ip address 10.19.8.97 255.255.255.248 ipv6 address 2001:DB8:ACAD:C::1/64 ipv6 enable
Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**	Enable Configure terminal interface Loopback0 ip address 209.165.201.1 255.255.255.224 ipv6 address FE80::1 link-local ipv6 address 2001:DB8:ACAD:209::1/64 ipv6 enable
Generar una clave de cifrado RSA Módulo de 1024 bits	Enable Configure terminal crypto key generate rsa general-keys modulus 1024

Tabla 3. Tabla de configuraciones realizada en R1_Paso 2_Parte 1

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

A continuación se adjunta la configuración realizada para cumplir con lo solicitado en el presente ítem.

Tarea	Especificación
Desactivar la búsqueda DNS.	Enable Configure terminal No ip domain-lookup
Nombre del switch **S1 o S2, según proceda**	Enable Configure terminal Hostname S1 Enable Configure terminal Hostname S2
Nombre de dominio	Enable Configure terminal Ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Enable Configure terminal Enable secret ciscoenpass
Contraseña de acceso a la consola	Enable Configure terminal Line console 0 Password ciscoconpass login
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	Enable Configure terminal Username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Enable Configure terminal Line vty 0 15 Login local

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Enable Configure terminal Line vty 0 15 Transport input ssh
Cifrar las contraseñas de texto no cifrado	Enable Configure terminal Service password-encryption
Configurar un MOTD Banner	Enable Configure terminal Banner motd & Bienvenido&
Generar una clave de cifrado RSA	Enable Configure terminal crypto key generate rsa general-keys modulus 1024

Tarea	Especificación
configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3	S1 Enable Configure terminal interface Vlan4 mac-address 00e0.8f88.7d02 ip address 10.19.8.98 255.255.255.248 ipv6 address FE80::98 link-local ipv6 address 2001:DB8:ACAD:C::98/64 ipv6 enable no shutdown S2 Enable Configure terminal interface Vlan4 mac-address 00d0.d3b4.b701 ip address 10.19.8.99 255.255.255.248 ipv6 address FE80::99 link-local ipv6 address 2001:DB8:ACAD:C::99/64 ipv6 enable no shutdown
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S1 Enable Configure terminal interface Vlan4 ip default-gateway 10.19.8.97 S2 Enable Configure terminal ip default-gateway 10.19.8.97

Tabla 4. Tabla de configuraciones realizadas en S1 y S2_Paso 3_Parte 1

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En la siguiente tabla podemos observar la configuración realizada para cumplir con lo solicitado en el presente ítem.

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1 Enable Configure terminal vlan 2 Name Bikes Vlan 3 Name Trikes Vlan 4 Name Management Vlan 5 Name Parking Vlan 6 Name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1 Enable Configure terminal interface FastEthernet0/1 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/2 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/5 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1 Enable Configure terminal interface Port-channel1 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/1 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk channel-protocol lacp channel-group 1 mode active interface FastEthernet0/2 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk channel-protocol lacp channel-group 1 mode active
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	Enable Configure terminal interface FastEthernet0/6 switchport access vlan 2 switchport mode access
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	Enable Configure terminal interface range FastEthernet 0/3 -4 switchport port-security switchport port-security maximum 3 interface range FastEthernet 0/6 -24 switchport port-security switchport port-security maximum 3

Tarea	Especificación
21	interface FastEthernet0/3 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown interface FastEthernet0/4 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown interface FastEthernet0/7 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown interface FastEthernet0/8 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown interface FastEthernet0/9 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown interface FastEthernet0/10 description DOWN-SECURITY switchport access vlan 5 switchport mode access switchport port-security switchport port-security maximum 3 shutdown

Tabla 5. Tabla de configuraciones realizadas en S1_Paso 4_Parte 1

Paso 5: Configure el S2.

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

A continuación se adjunta la configuración realizada para cumplir con lo solicitado en el presente ítem.

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1 Enable Configure terminal vlan 2 Name Bikes Vlan 3 Name Trikes Vlan 4 Name Management Vlan 5 Name Parking Vlan 6 Name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S1 Enable Configure terminal interface FastEthernet0/1 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/2 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/5 switchport trunk native vlan 6 switchport trunk encapsulation dot1q switchport mode trunk

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S2: Enable Configure terminal interface Port-channel1 switchport trunk encapsulation dot1q switchport mode trunk interface FastEthernet0/1 switchport trunk encapsulation dot1q switchport mode trunk channel-protocol lacp channel-group 1 mode passive interface FastEthernet0/2 switchport trunk encapsulation dot1q switchport mode trunk channel-protocol lacp channel-group 1 mode passive
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	Enable Configure terminal interface FastEthernet0/18 switchport access vlan 3 switchport mode access switchport port-security switchport port-security maximum 3
Configure port-security en los access ports permite 3 MAC addresses	Enable Configure terminal interface range FastEthernet 0/3 -24 switchport port-security switchport port-security maximum 3 interface range GigabitEthernet 0/1 -2 switchport port-security switchport port-security maximum 3

Tarea	Especificación
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	Enable Configure terminal interface range FastEthernet 0/3 -17 description DOWN-SECURITY shutdown interface range FastEthernet 0/19 - 24 description DOWN-SECURITY shutdown interface range GigabitEthernet 0/1 - 2 description DOWN-SECURITY shutdown

Tabla 6. Tabla de configuraciones realizadas en S2_Paso 5_Parte 1

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	Enable Configure terminal ip route 0.0.0.0 0.0.0.0 Loopback0 ipv6 route ::/0 Loopback0

Tarea	Especificación
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	Enable Configure terminal ip dhcp pool VLAN2 network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 domain-name ccna-a.net ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	Enable Configure terminal ip dhcp pool VLAN3 network 10.19.8.64 255.255.255.224 default-router 10.19.8.65 domain-name ccna-a.net ip dhcp excluded-address 10.19.8.65 10.19.8.84

Tabla 7. Tabla de configuraciones realizadas en R1_Paso 1_Parte 2

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**.

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	0002.4A3D.CA03

PC-A Network Configuration	
Dirección IP	10.19.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 8. Tabla de configuraciones realizadas en PCA_Paso 2_Parte 2

Configuración de red de PC-B	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	000A.411D.D75E
Dirección IP	10.19.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B::1

Tabla 9.Tabla de configuraciones realizadas en PCB_Paso 2_Parte 2

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:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso!!*
		IPv6	2001:db8:acad:a: :1	*Exitoso!!*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Exitoso!!*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b: :1	*Exitoso!!*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Exitoso!!*
		IPv6	2001:db8:acad:c: :1	*Exitoso!!*
	S1, VLAN 4	Dirección	10.19.8.98	*Exitoso!!*
		IPv6	2001:db8:acad:c: :98	*Falta el gateway por defecto en IPV6 – No exitoso!!*
	S2, VLAN 4	Dirección	10.19.8.99.	*Exitoso!!*
		IPv6	2001:db8:acad:c: :99	*Falta el gateway por defecto en IPV6 – No exitoso!!*
	PC-B	Dirección	IP address will vary.	
		IPv6	2001:db8:acad:b: :50	*Exitoso!!*
	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso!!*
		IPv6	2001:db8:acad:209: :1	*Exitoso!!*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso!!*
		IPv6	2001:db8:acad:209: :1	*Exitoso!!*
	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso!!*
		IPv6	2001:db8:acad:a: :1	*Exitoso!!*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Exitoso!!*
		IPv6	2001:db8:acad:b: :1	*Exitoso!!*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Exitoso!!*
		IPv6	2001:db8:acad:c: :1	*exitoso!!*
	S1, VLAN 4	Dirección	10.19.8.98	*Exitoso!!*
		IPv6	2001:db8:acad:c: :98	*Falta el gateway por defecto en IPV6 – No exitoso!!*
	S2, VLAN 4	Dirección	10.19.8.99.	*Exitoso!!*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c: :99	*Falta el gateway por defecto en IPV6 – No exitoso!!*

Tabla 10. Tabla de direcciones para verificación de conectividad_Paso 2_Parte 3

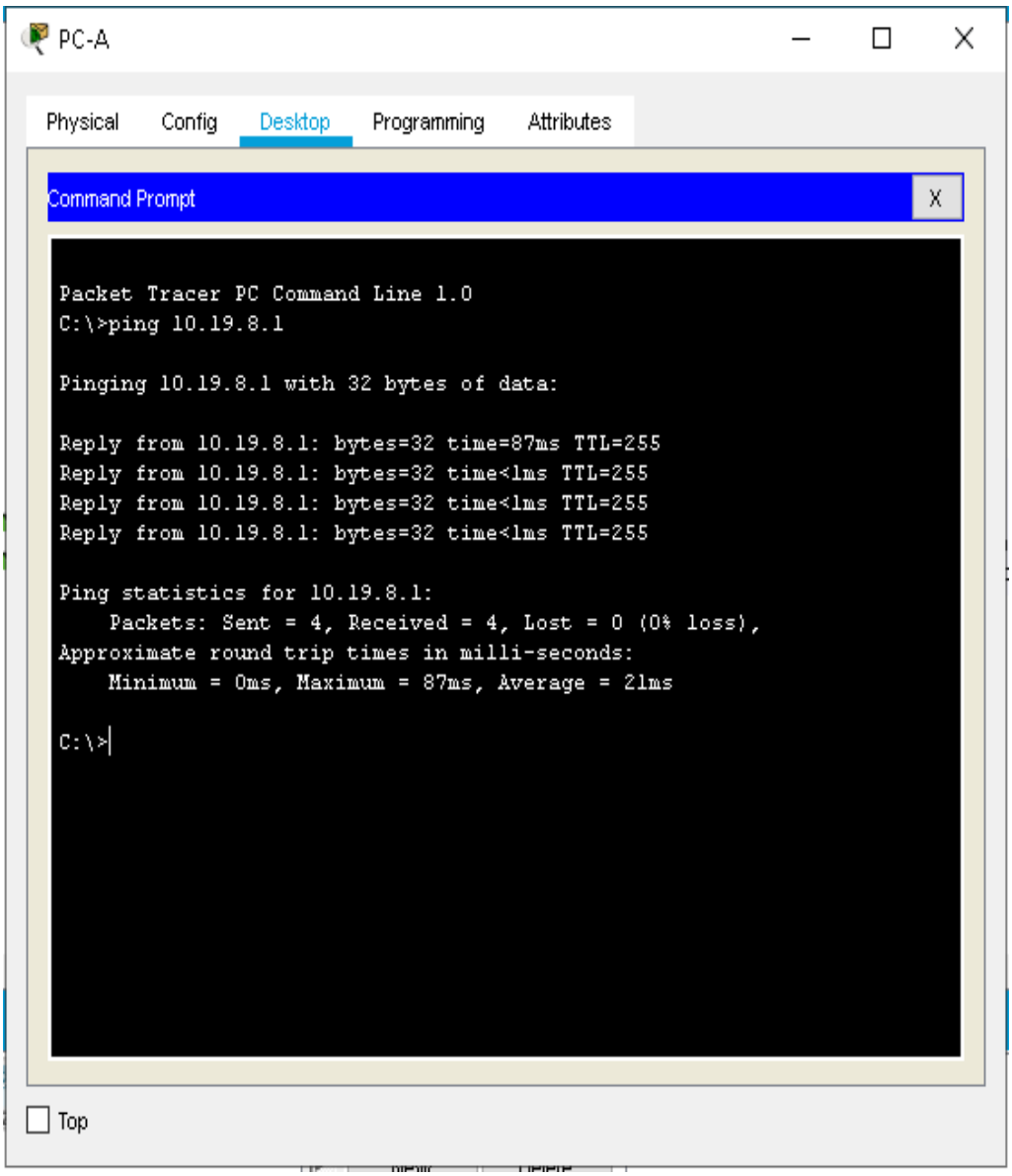


Figura 3. ping de PC-A a R1-G0/0/1.2_10.19.8.1_OK

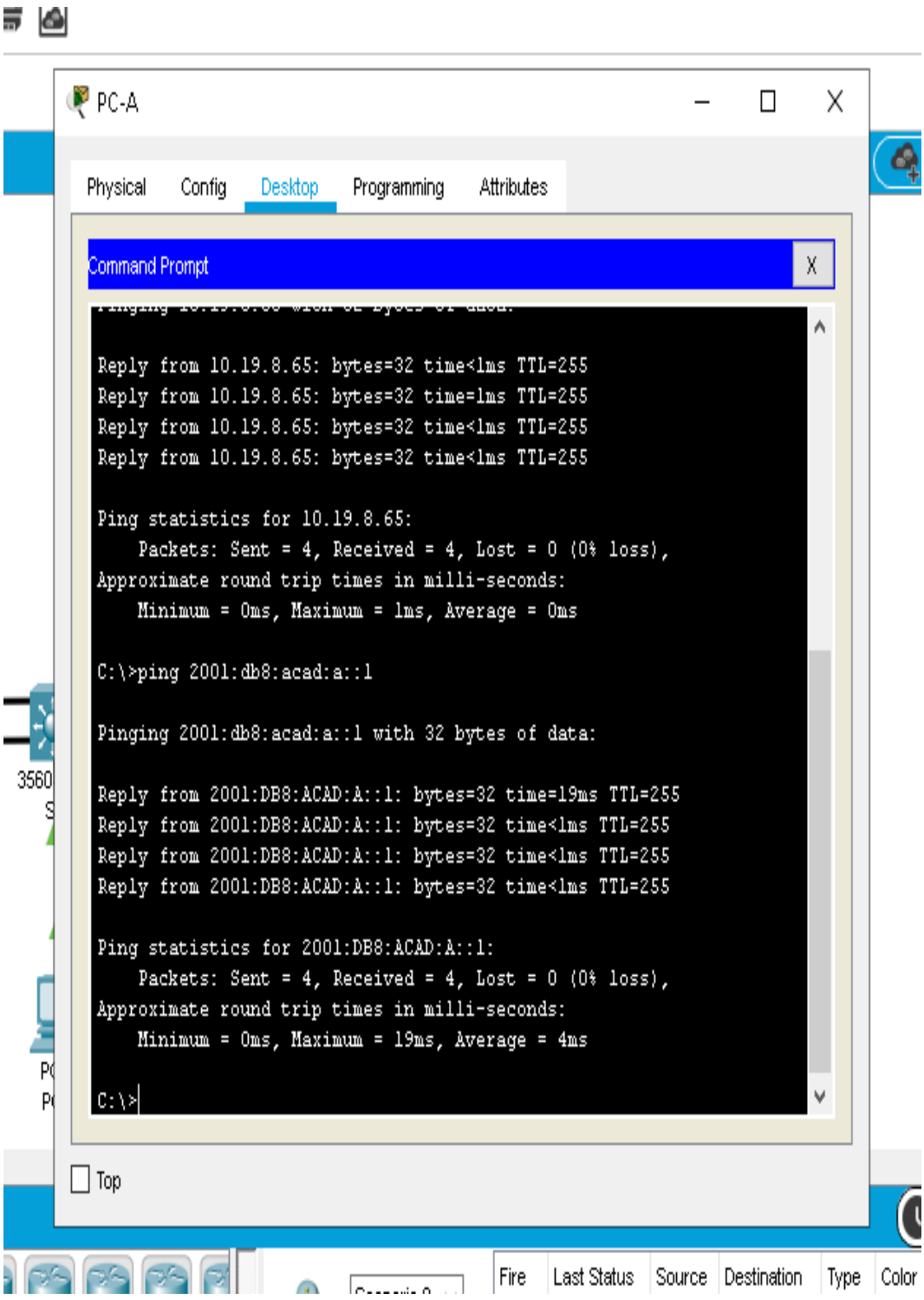


Figura 4. ping de PC-A a R1-G0/0/1.2_IPv6_OK

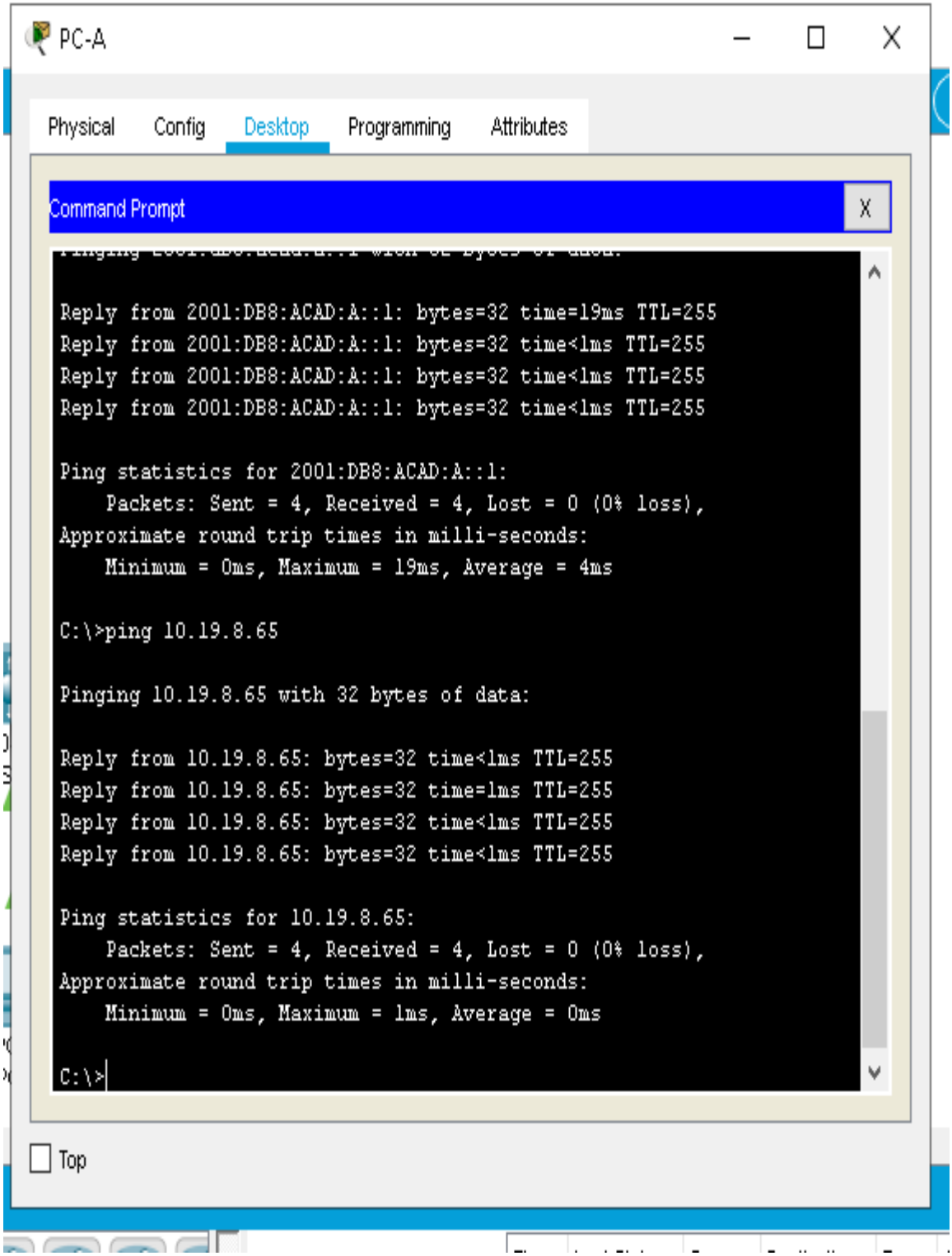


Figura 5. ping de PC-A a R1-G0/0/1.3_10.19.8.65_OK

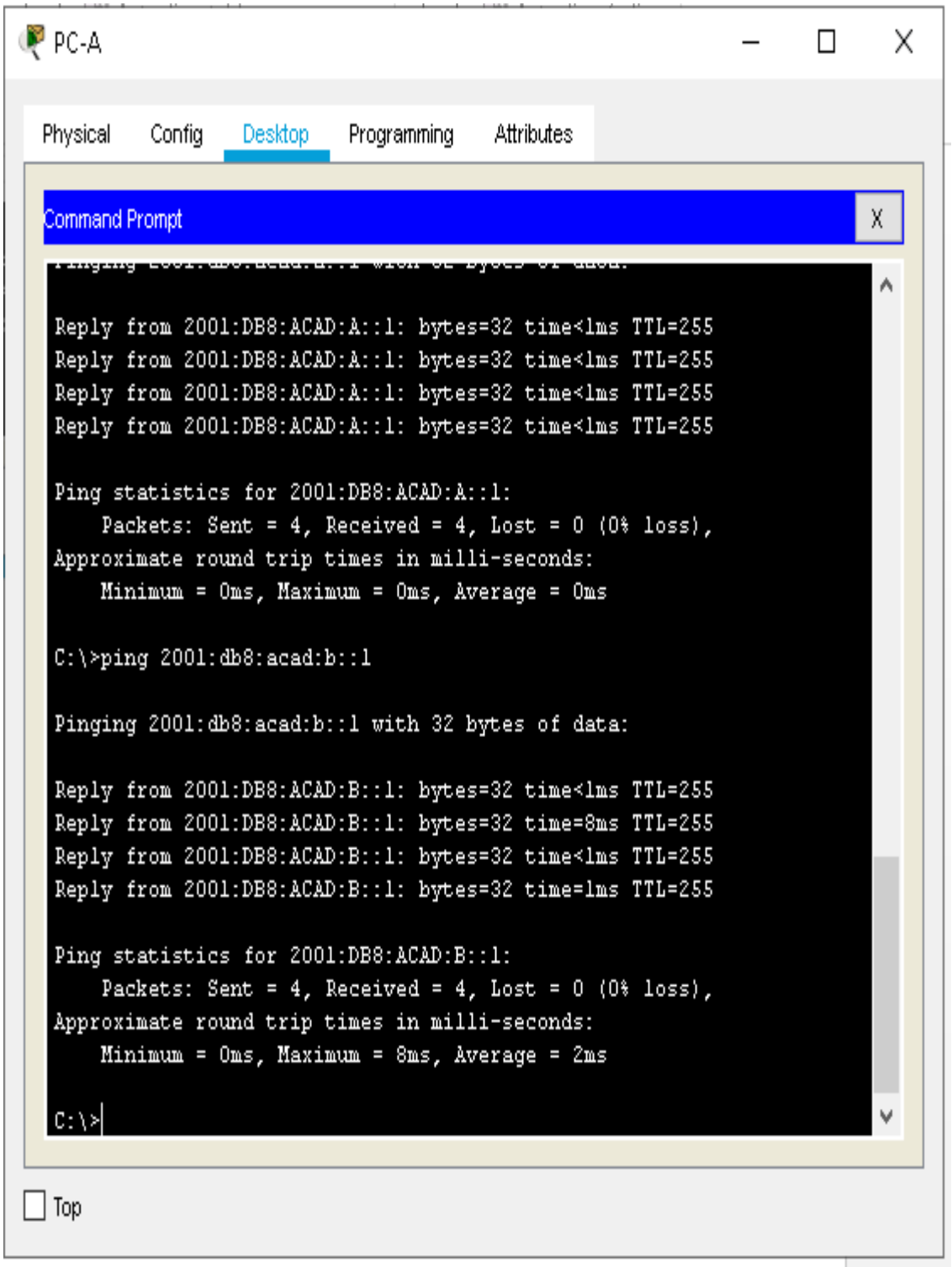


Figura 6. ping de PC-A a R1-G0/0/1.3_IPv6_OK

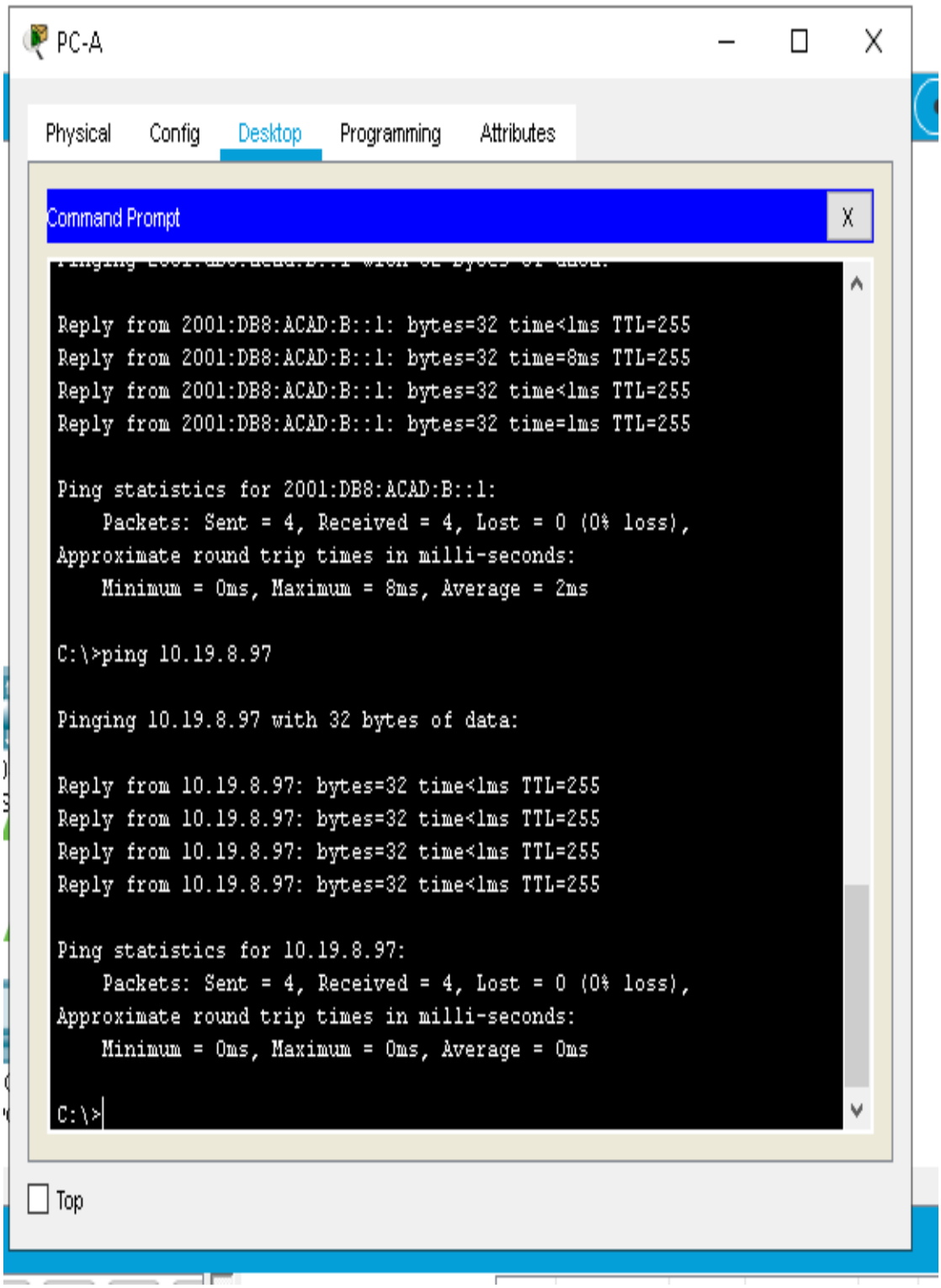


Figura 7. ping de PC-A a R1-G0/0/1.4_10.19.8.97_OK

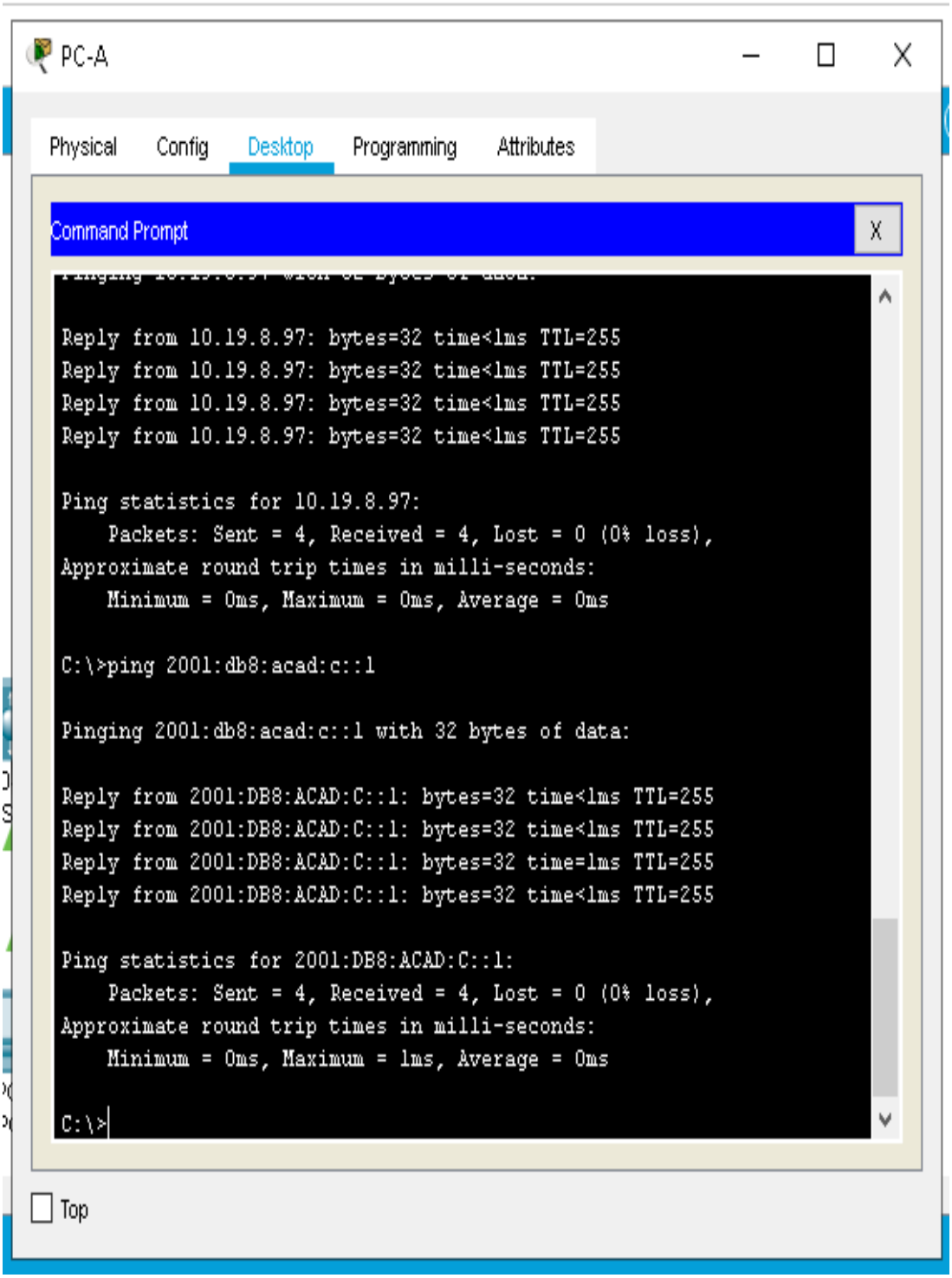


Figura 8. ping de PC-A a R1-G0/0/1.4_IPv6_OK

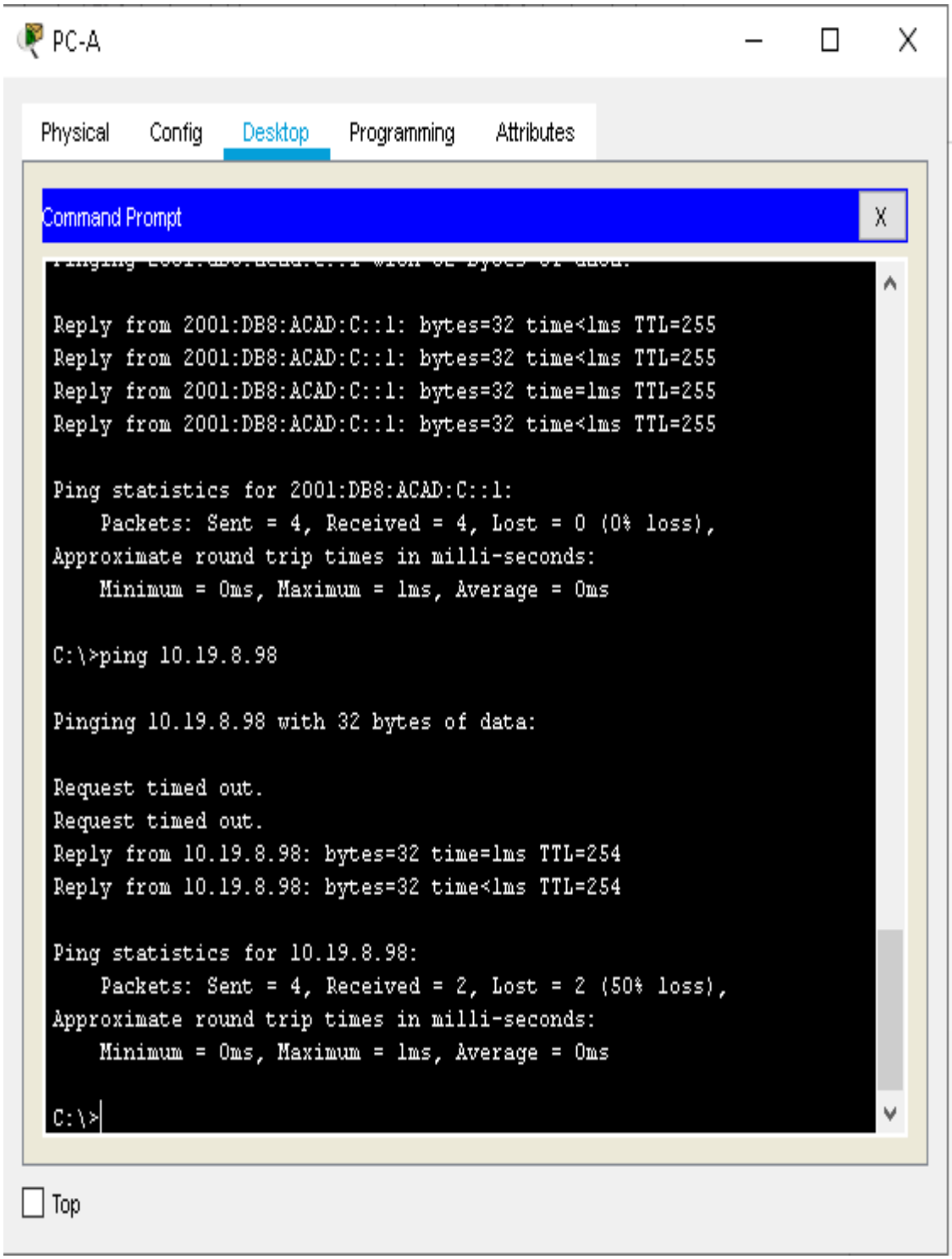


Figura 9. ping de PC-A a S1, VLAN 4_10.19.8.98_OK

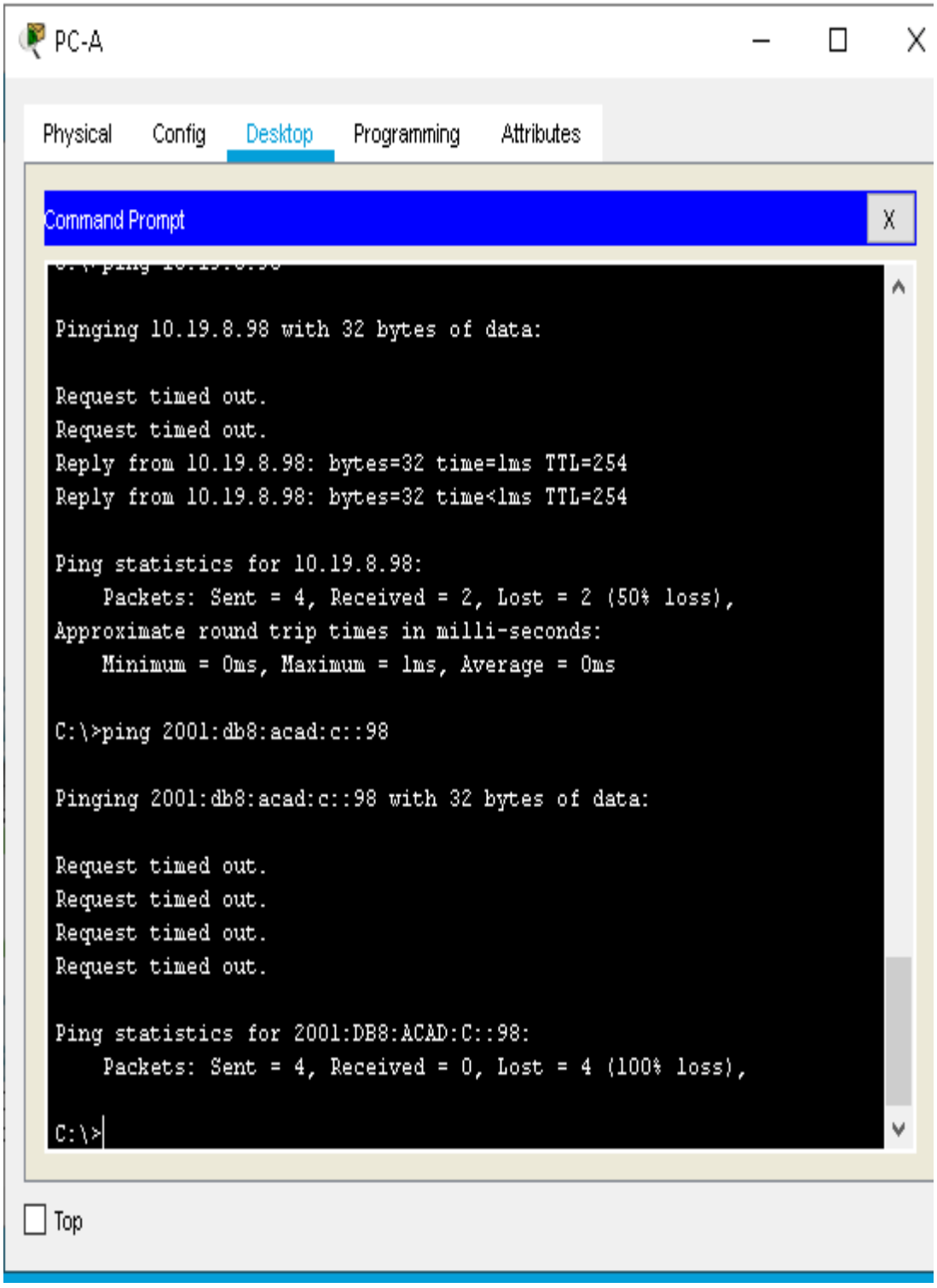


Figura 10. ping de PC-A a S1, VLAN 4_IPv6_FALLA

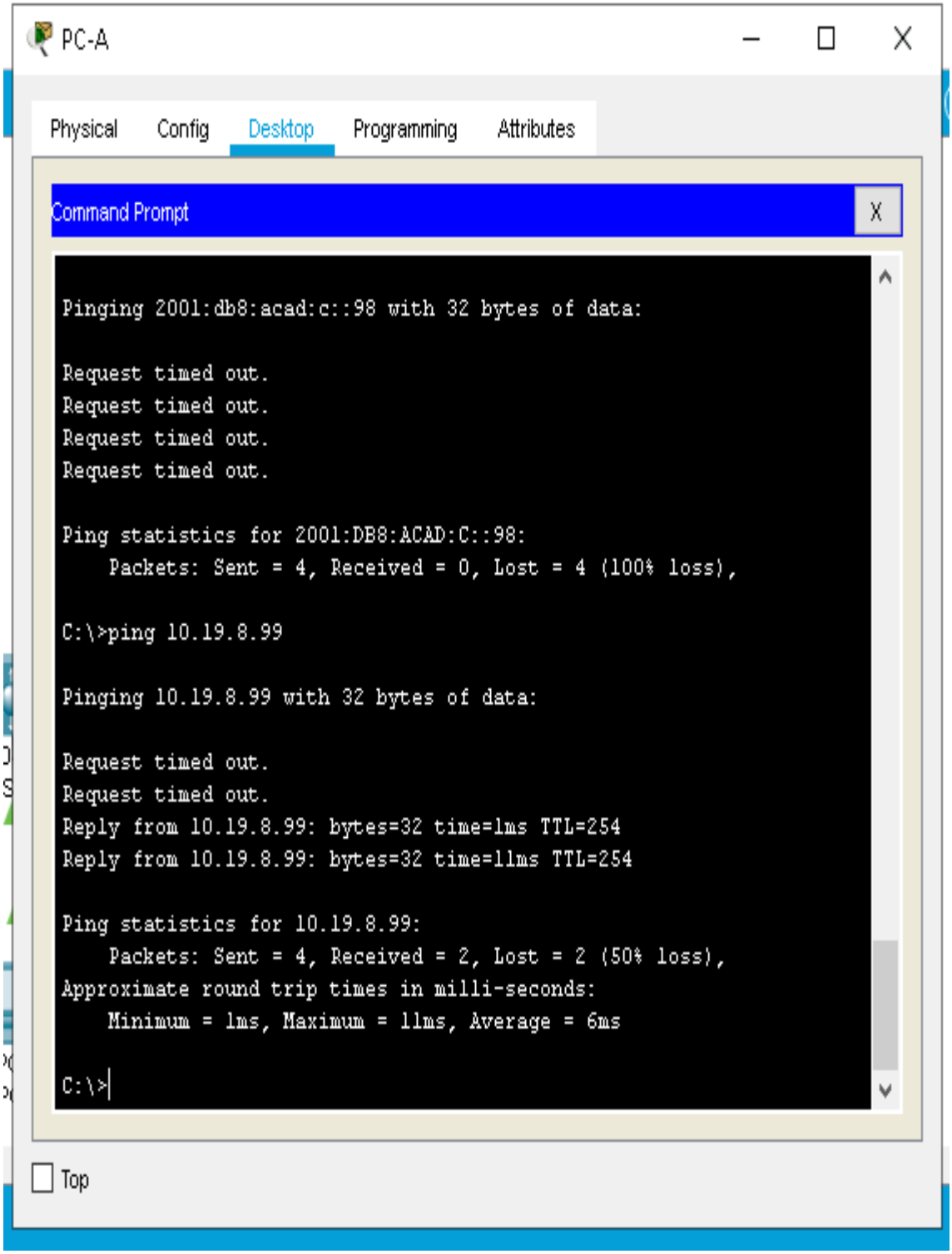


Figura 11. ping de PC-A a S2, VLAN 4_10.19.8.99_OK

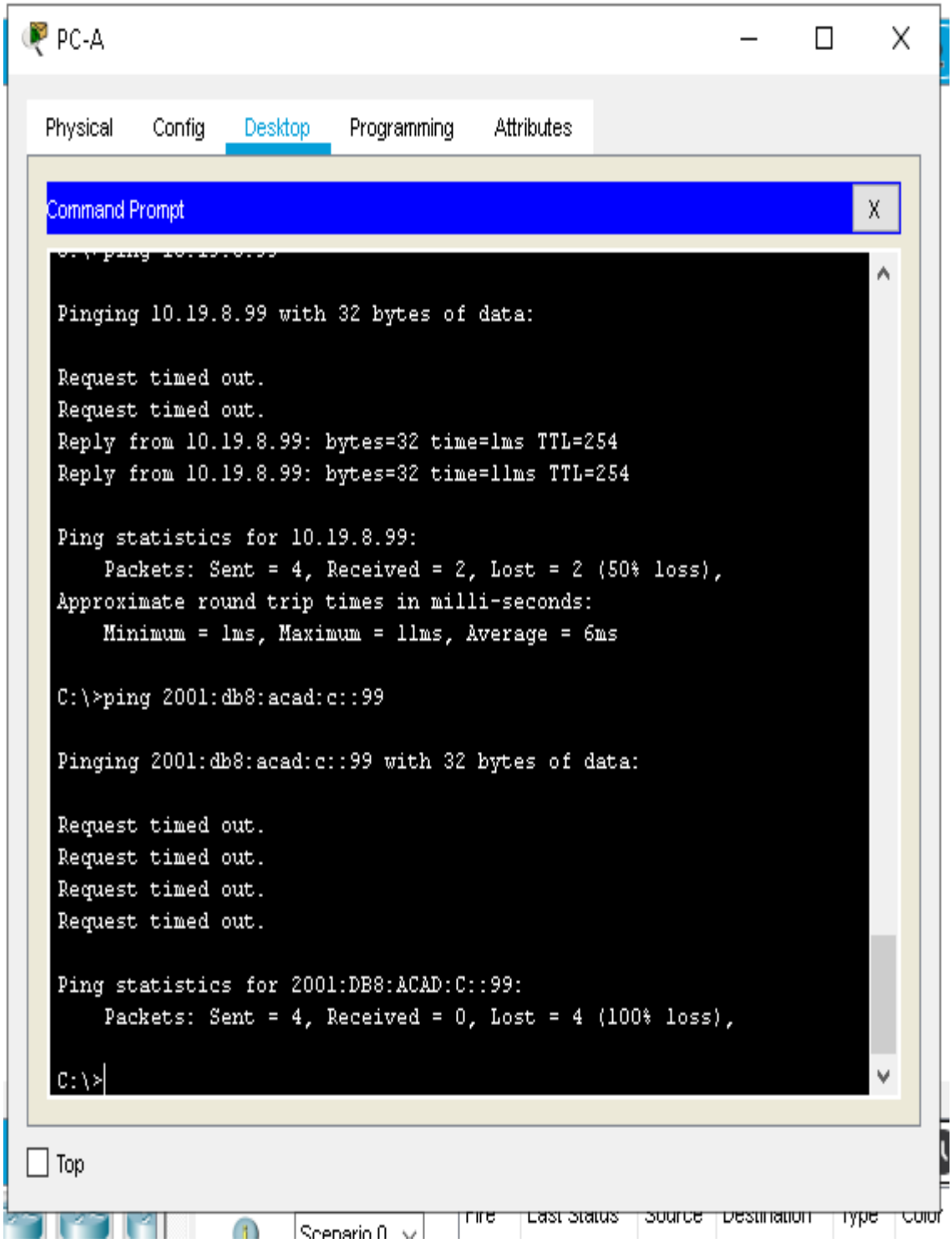


Figura 12. ping de PC-A a S2, VLAN 4_IPv6_FALLA

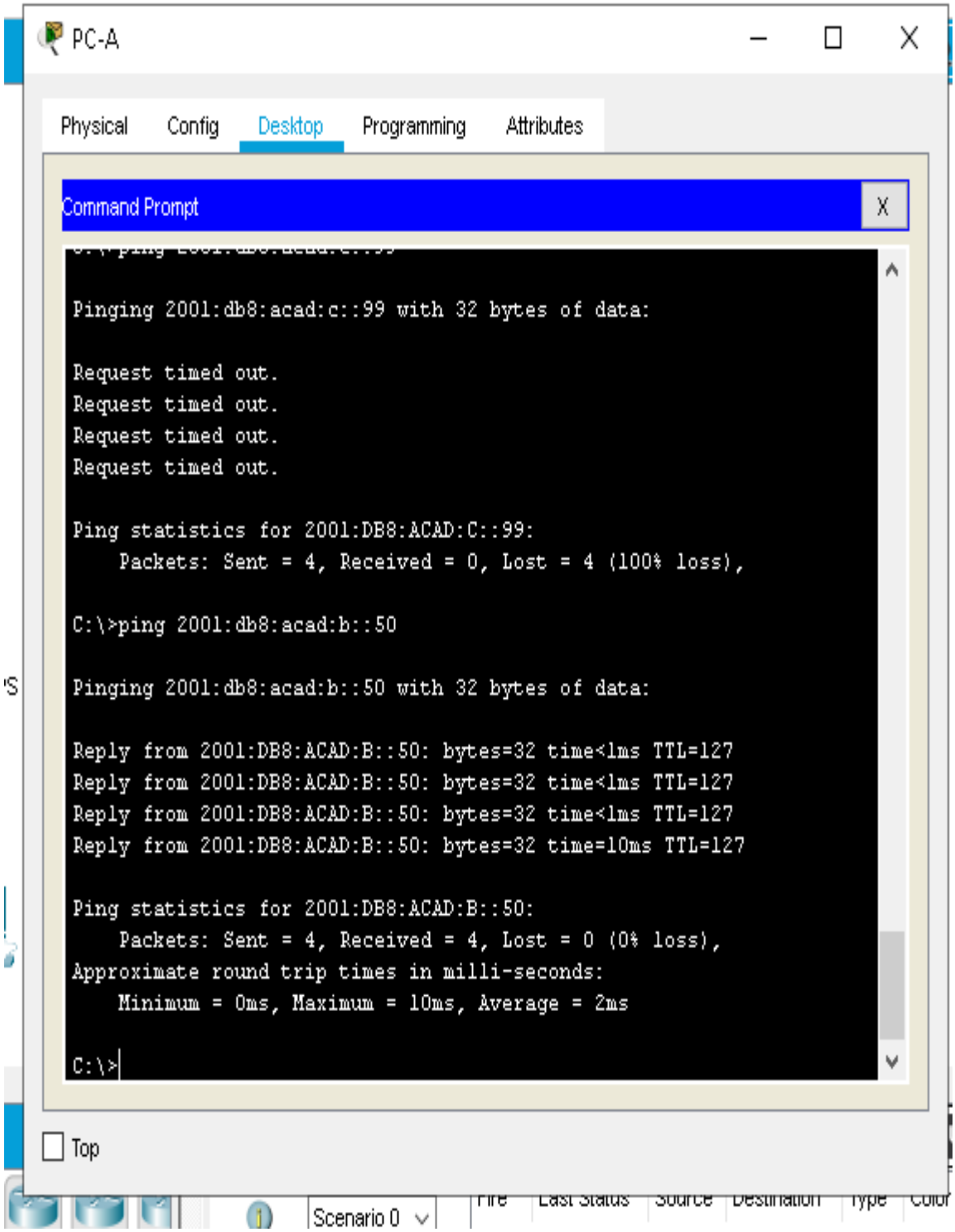


Figura 13. . ping de PC-A a PC-B_IPv6_OK

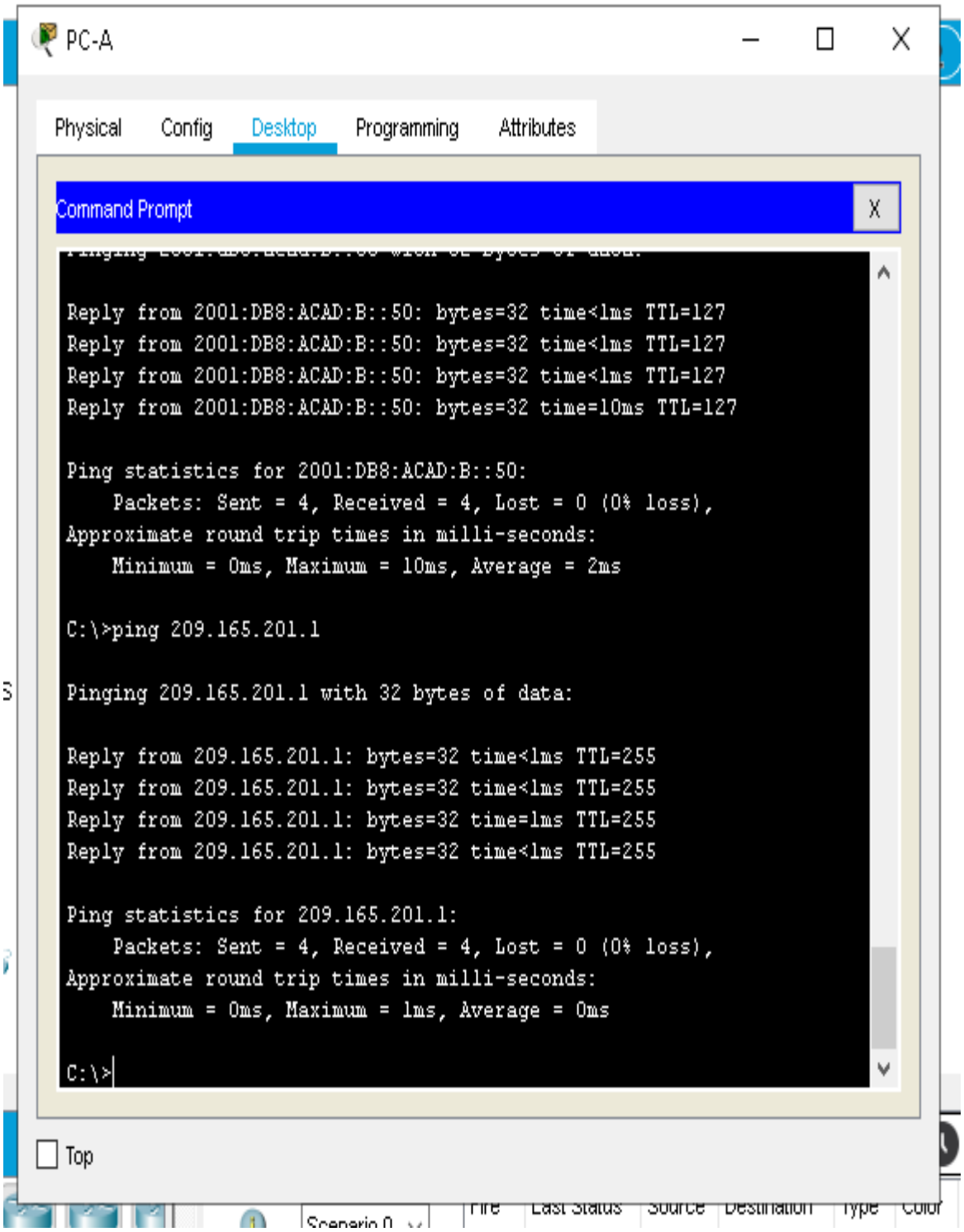


Figura 14. ping de PC-A a R1 Bucle 0_209.165.201.1

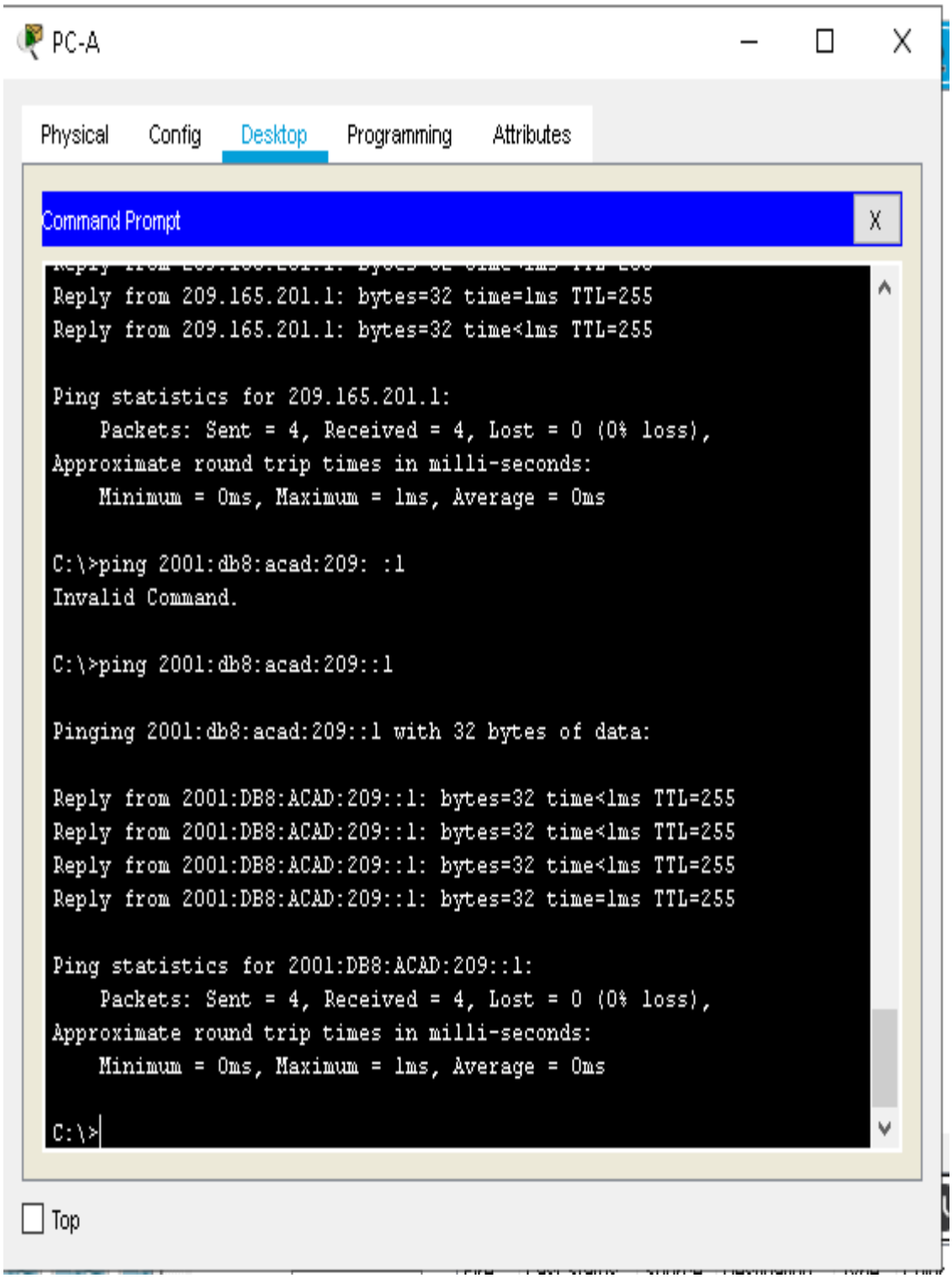


Figura 15. ping de PC-A a R1 Bucle 0_IPv6_FALLA

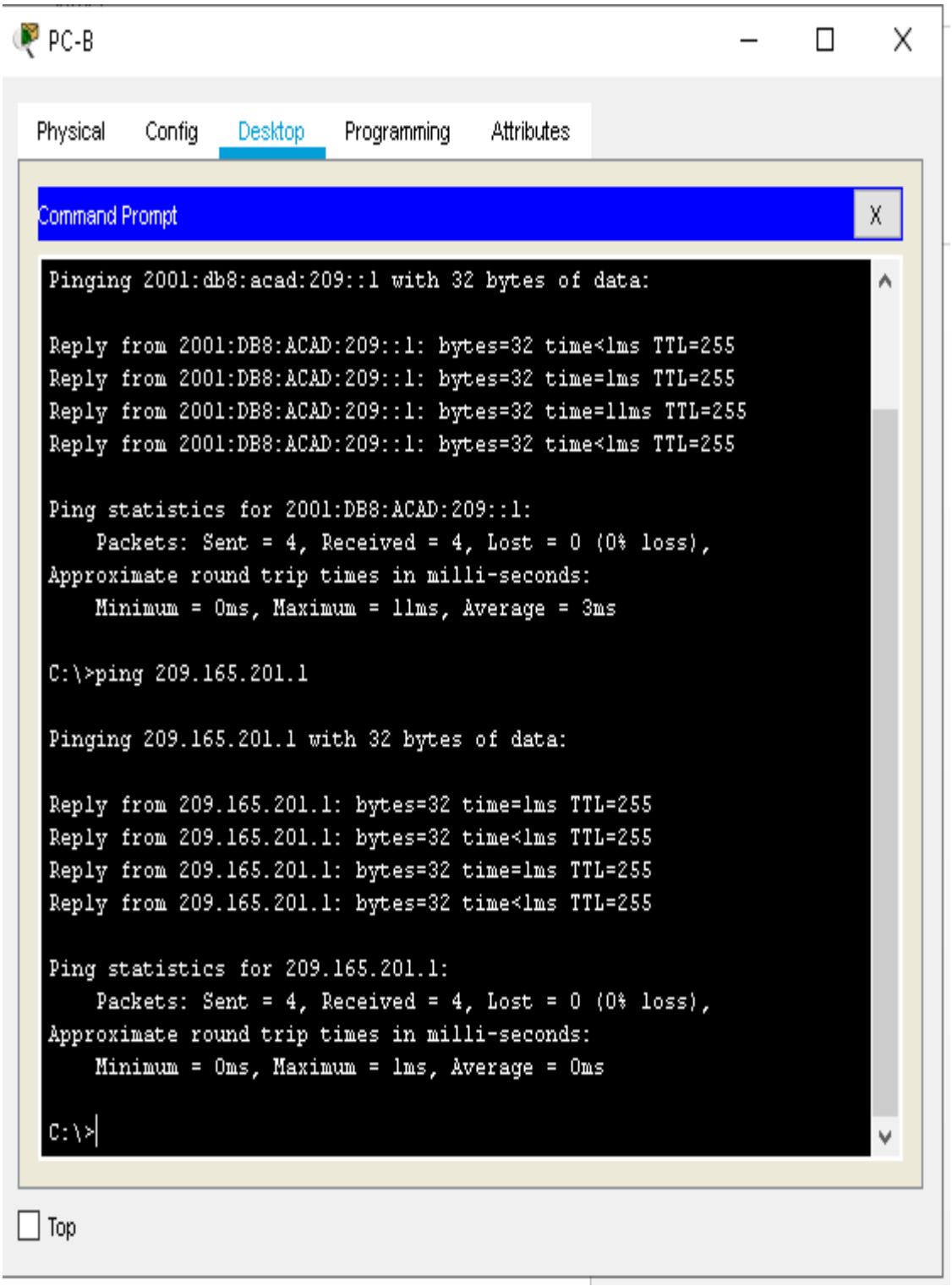


Figura 16. ping de PC-B a R1 Bucle 0_209.165.201.1_OK

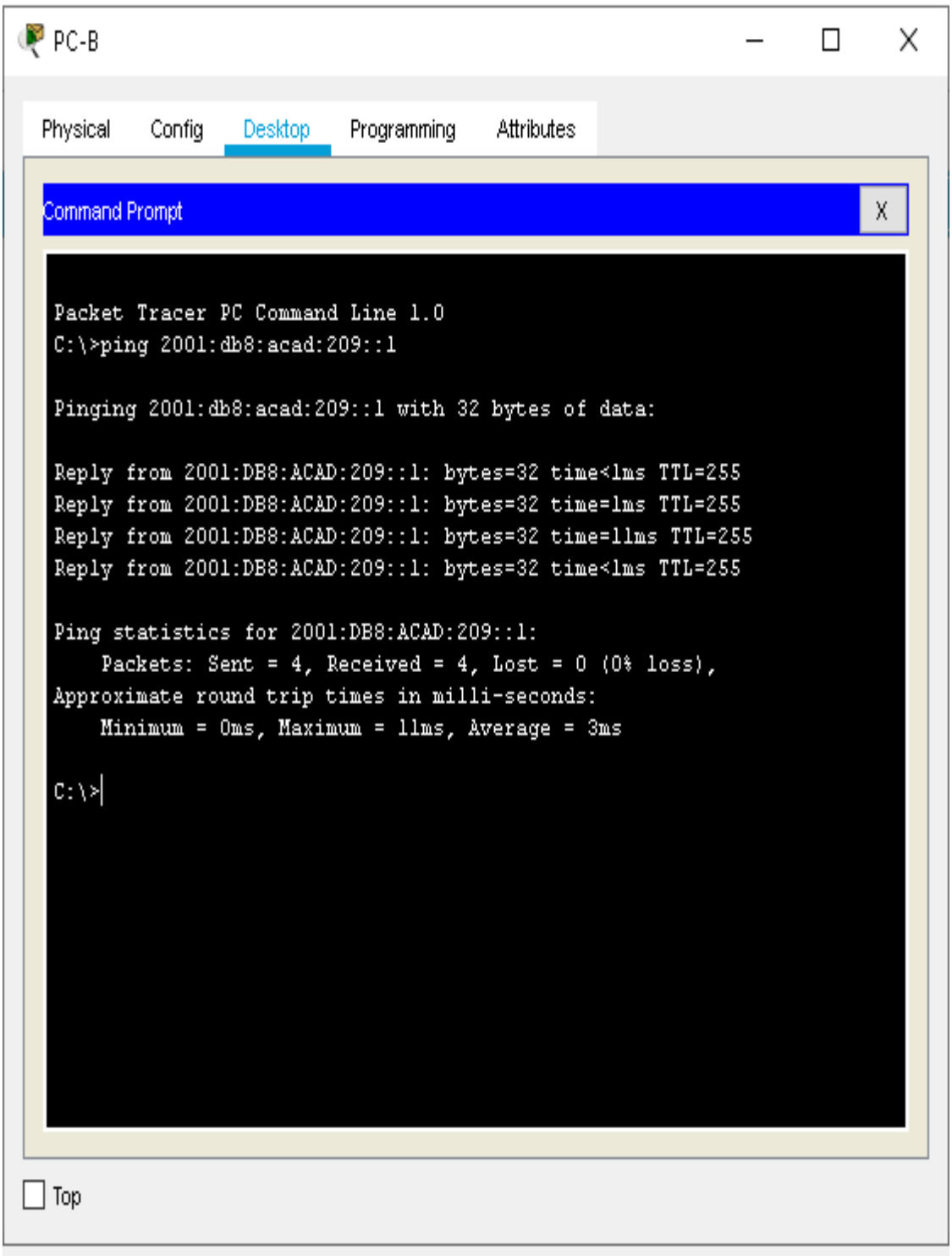


Figura 17. ping de PC-B a R1 Bucle 0_IPv6_OK

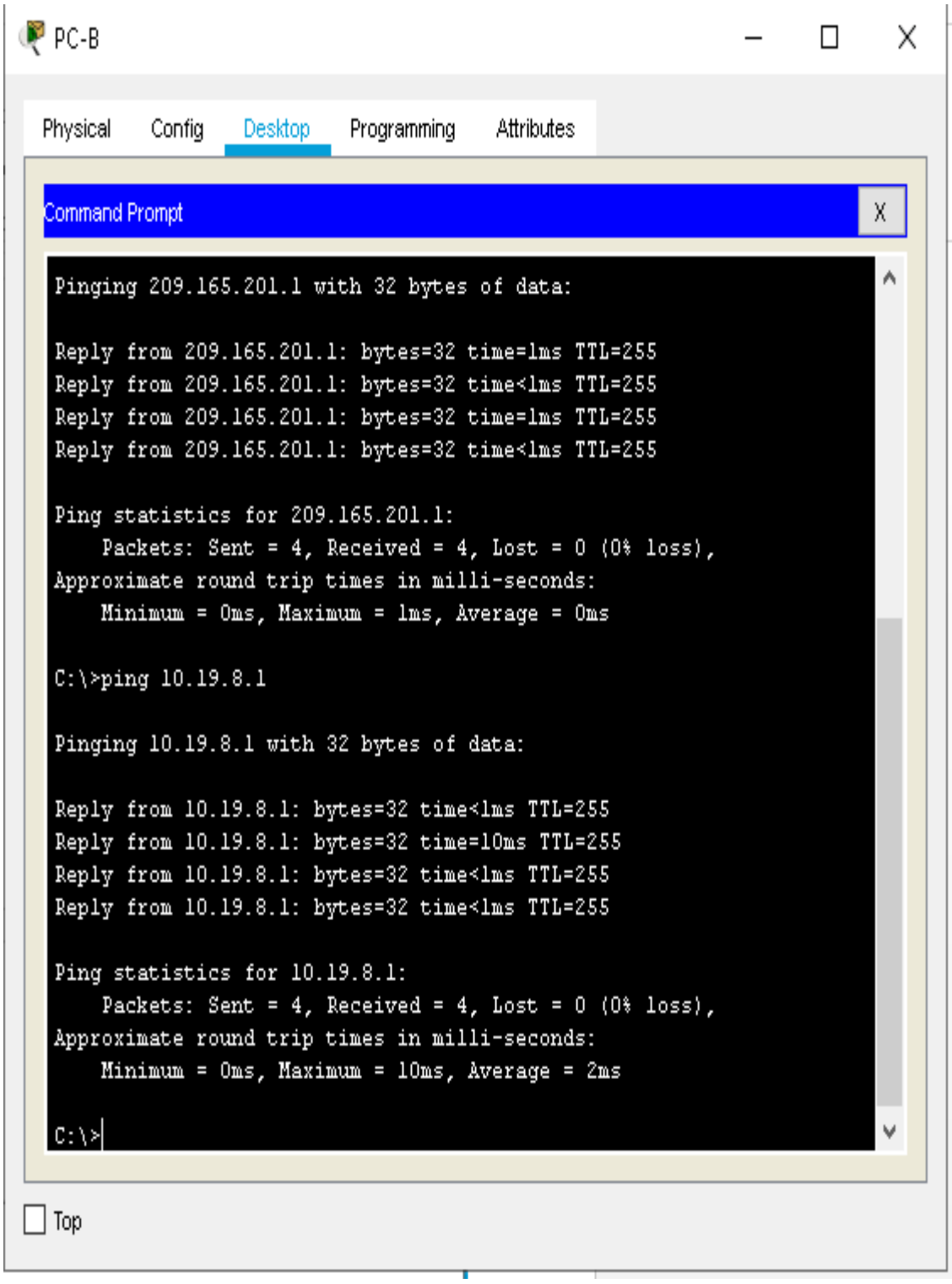


Figura 18. ping de PC-B a R1-G0/0/1.2_10.19.8.1_OK

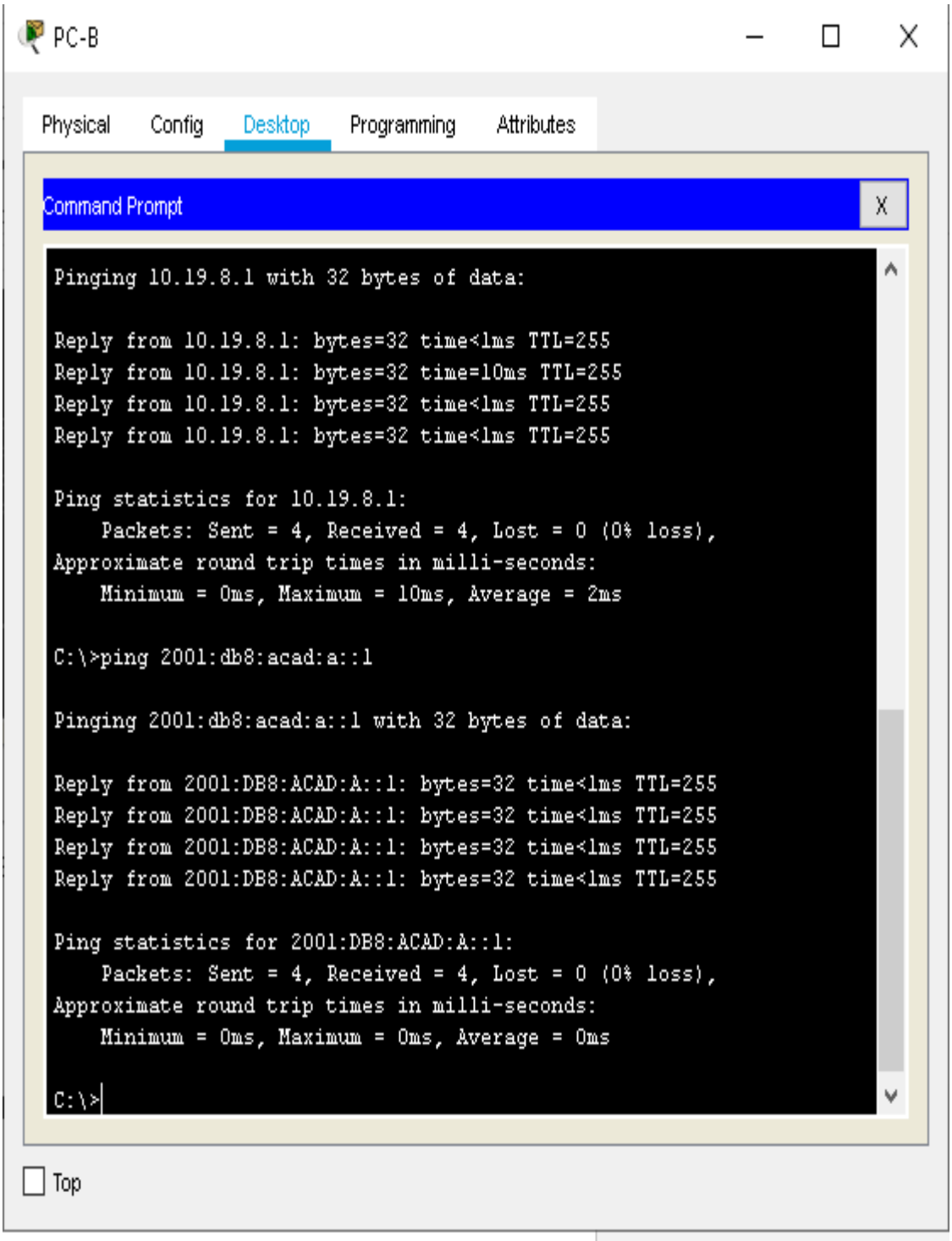


Figura 19. ping de PC-B a R1-G0/0/1.2_IPv6_OK

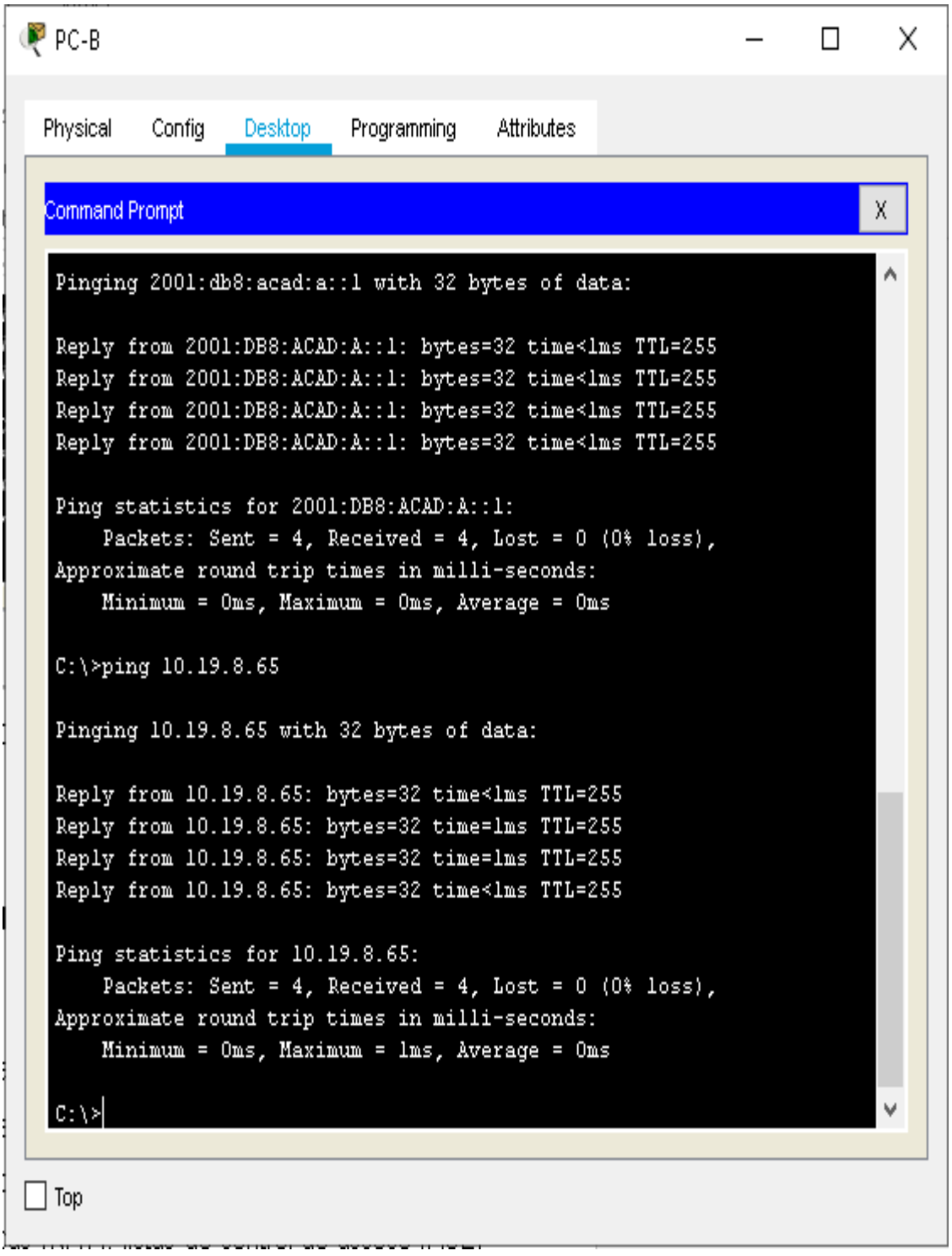


Figura 20.ping de PC-B a R1-G0/0/1.3_10.19.8.65_OK

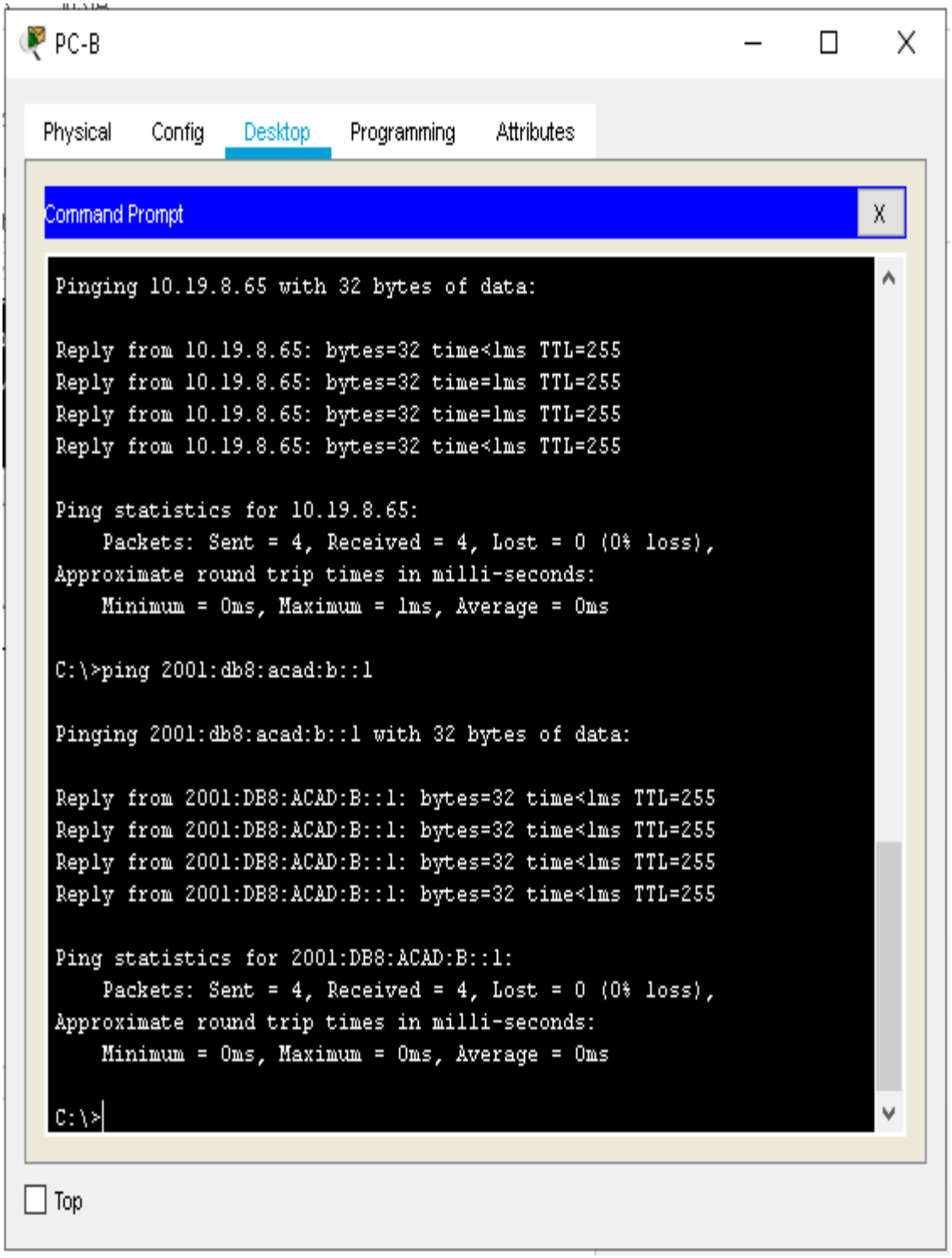


Figura 21. ping de PC-B a R1-G0/0/1.3_IPv6_OK

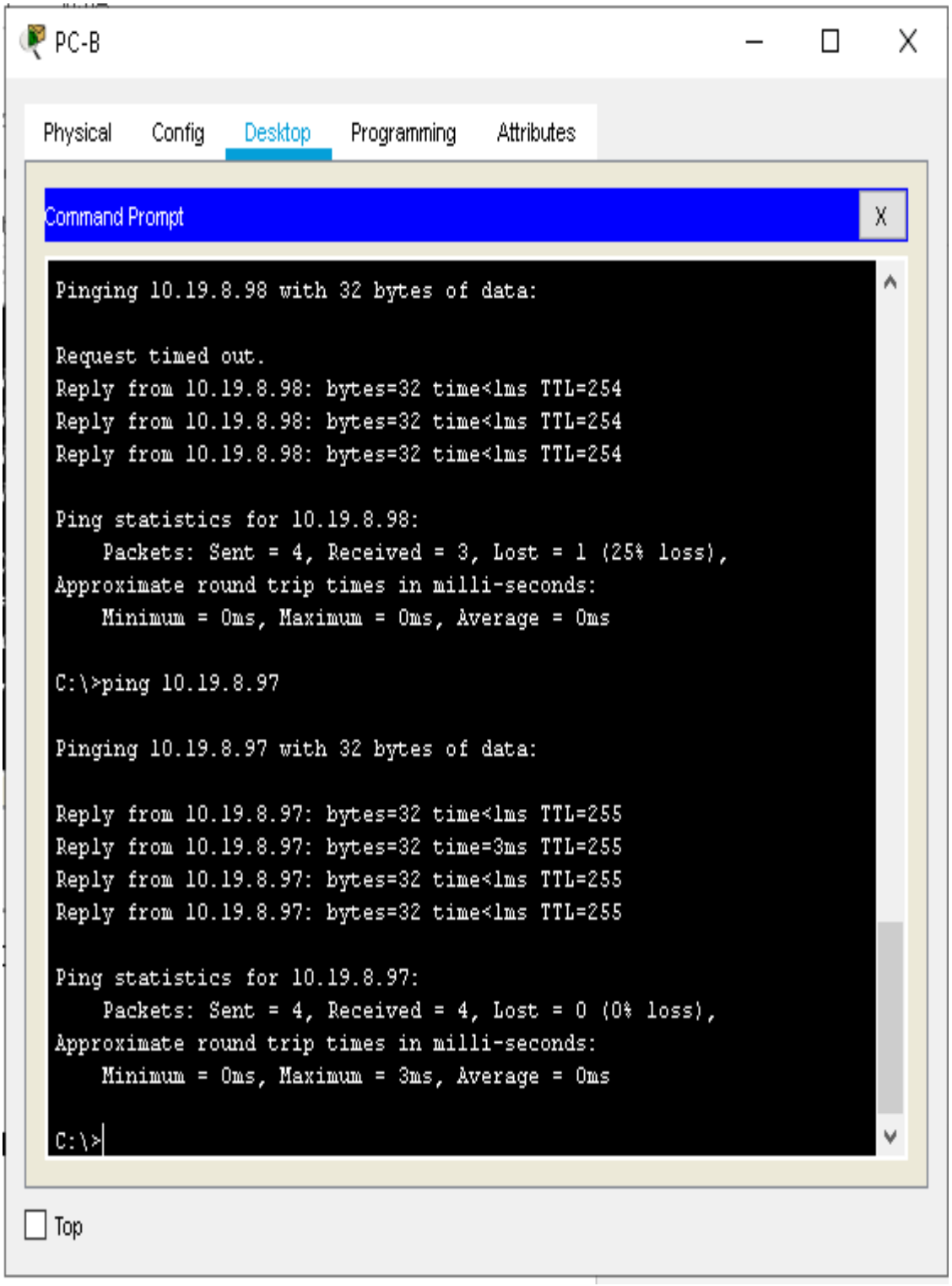


Figura 22. ping de PC-B a R1-G0/0/1.4_10.19.8.97_OK

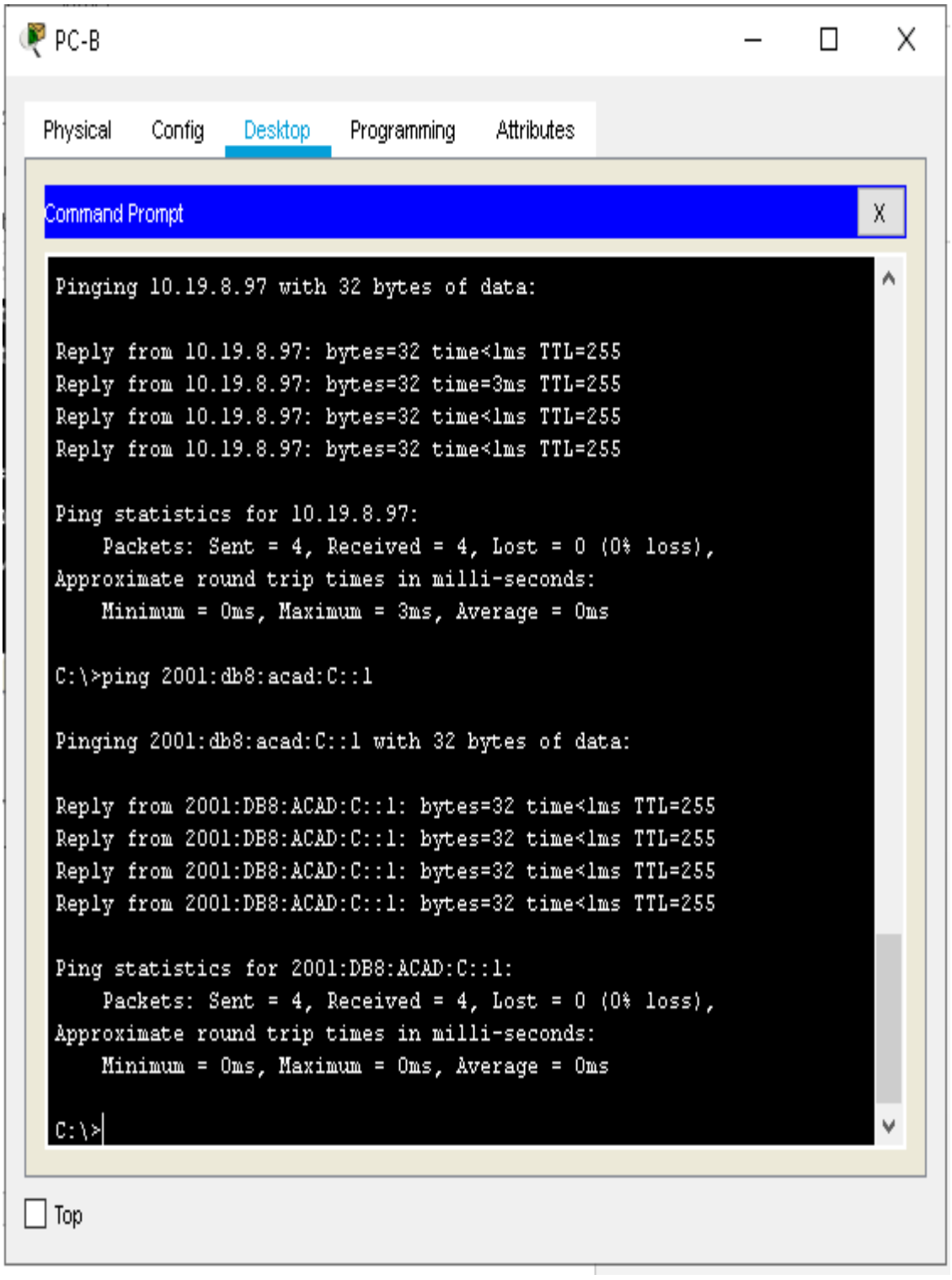


Figura 23. ping de PC-B a R1-G0/0/1.4_IPv6_OK

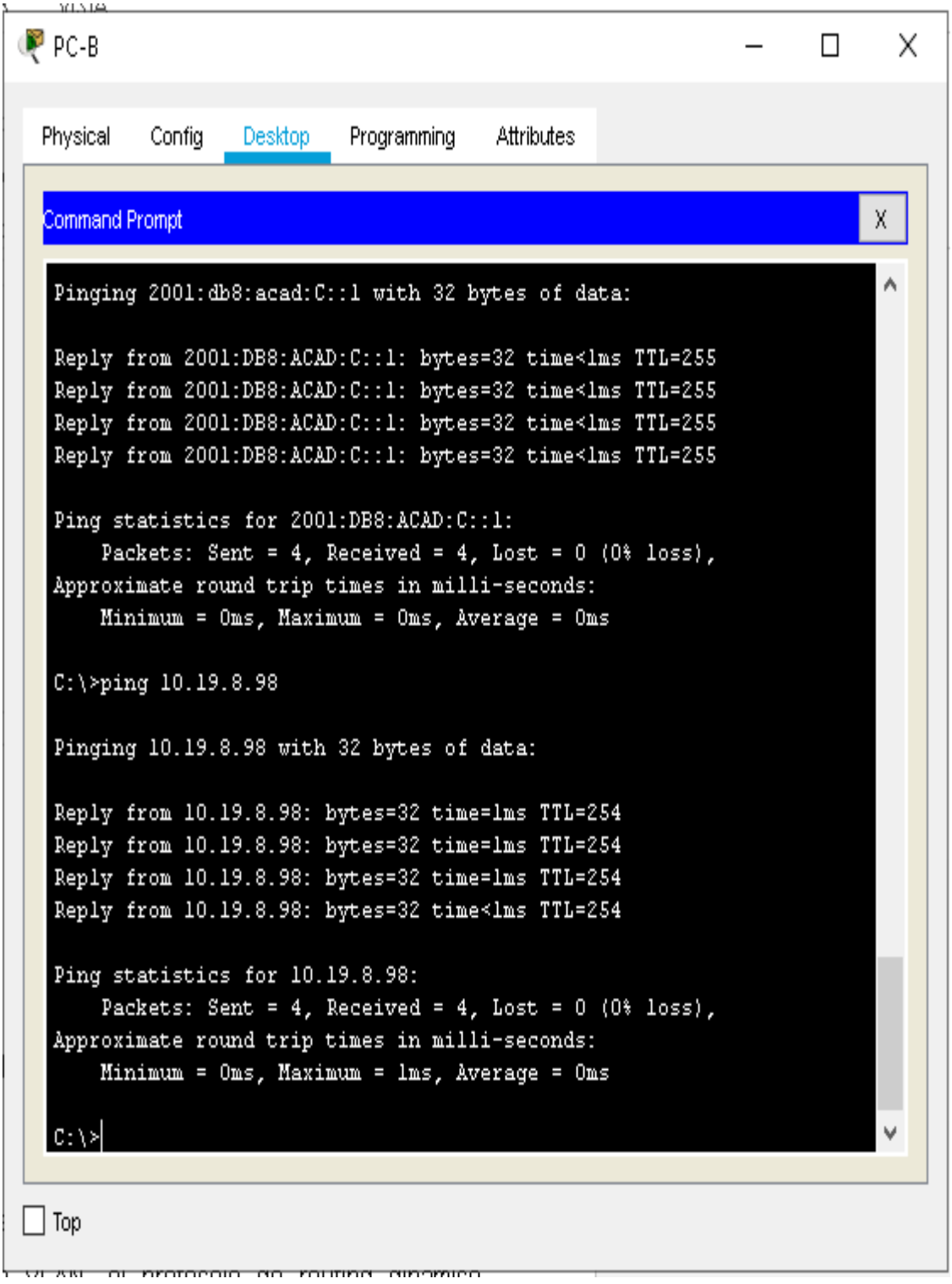


Figura 24. ping de PC-B a S1 VLAN 4_10.19.8.98_OK

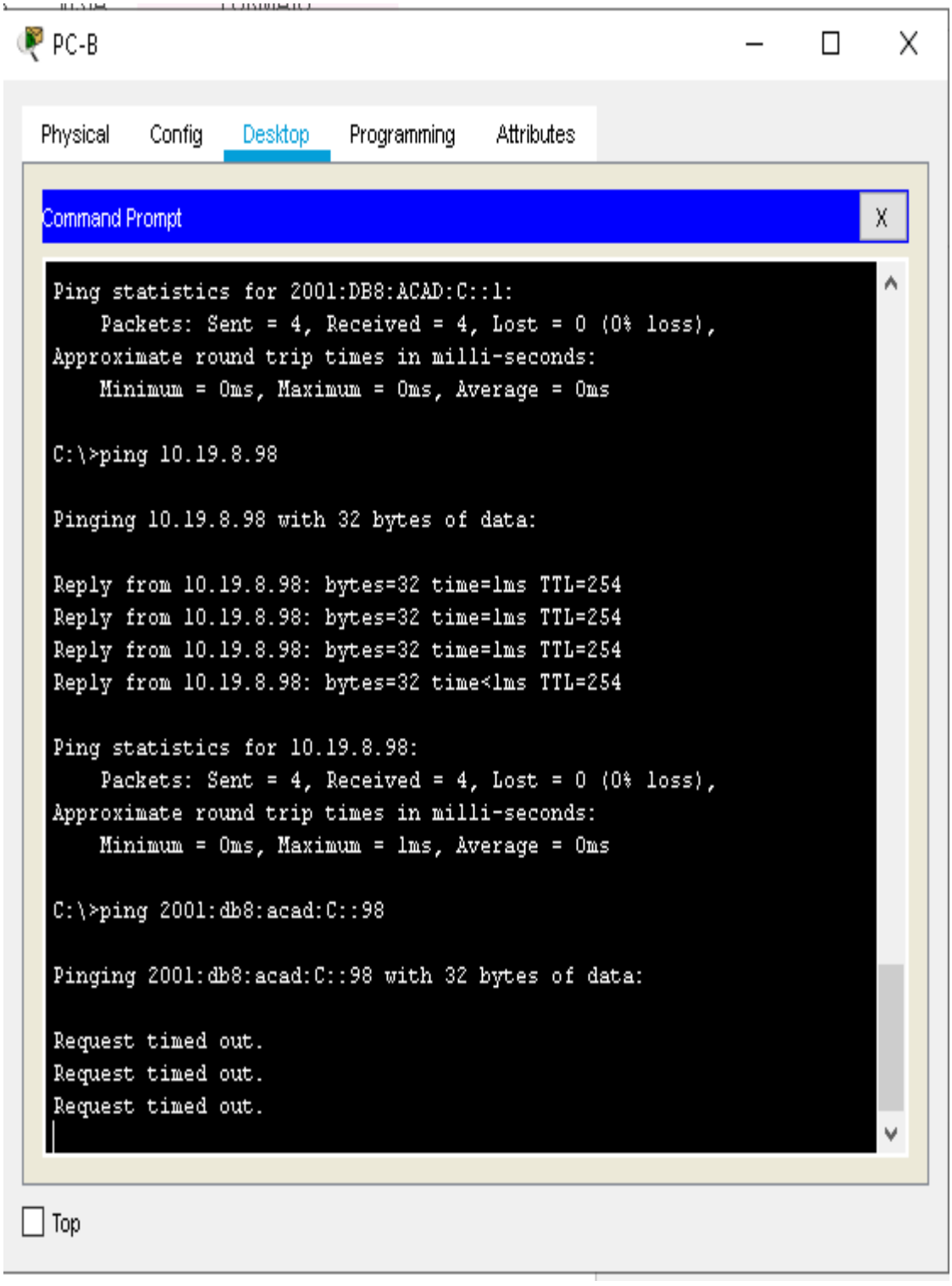


Figura 25. ping de PC-B a S1 VLAN 4_IPv6_FALLA

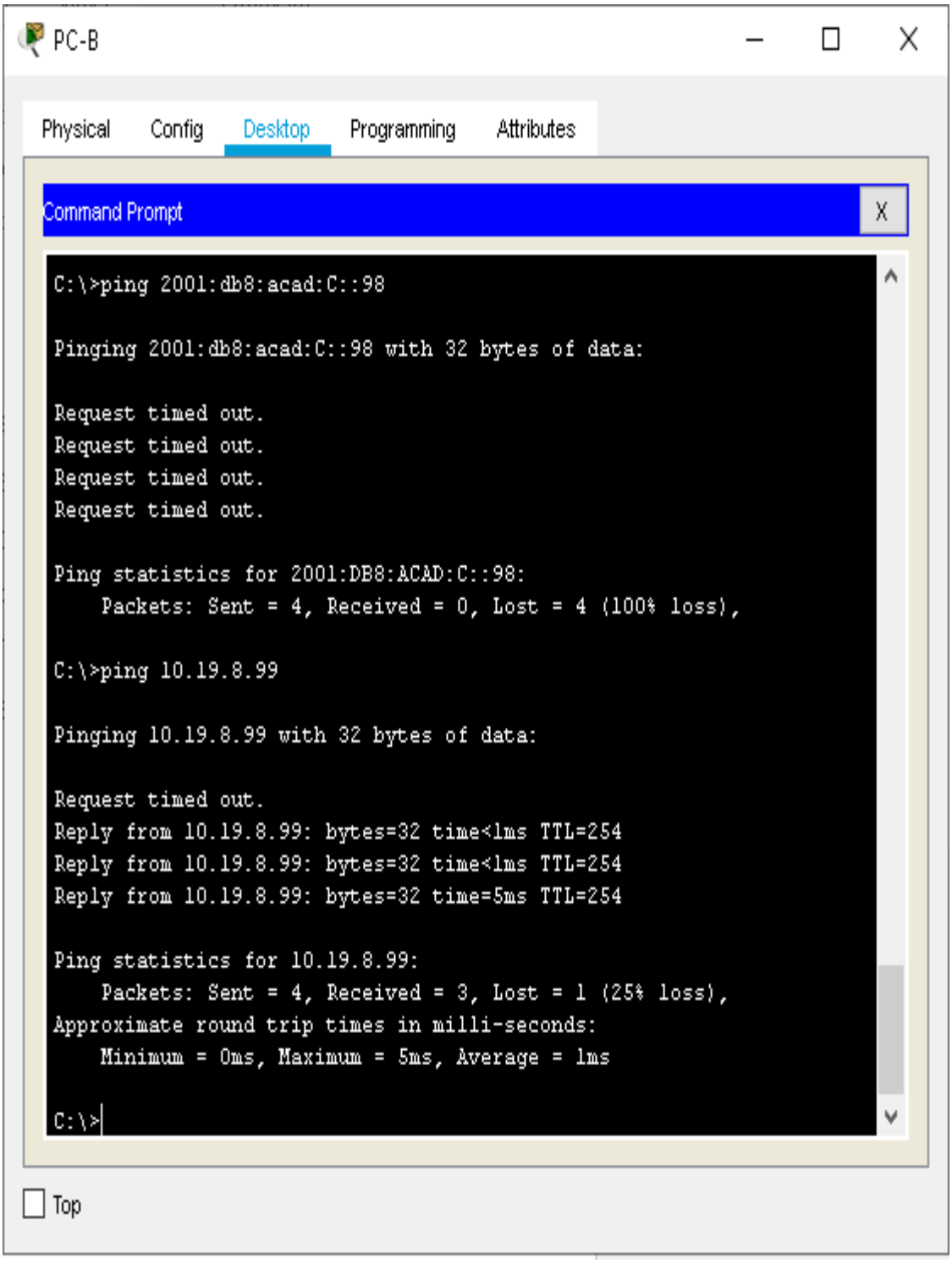


Figura 26. ping de PC-B a S1 VLAN 4_10.19.8.99_OK

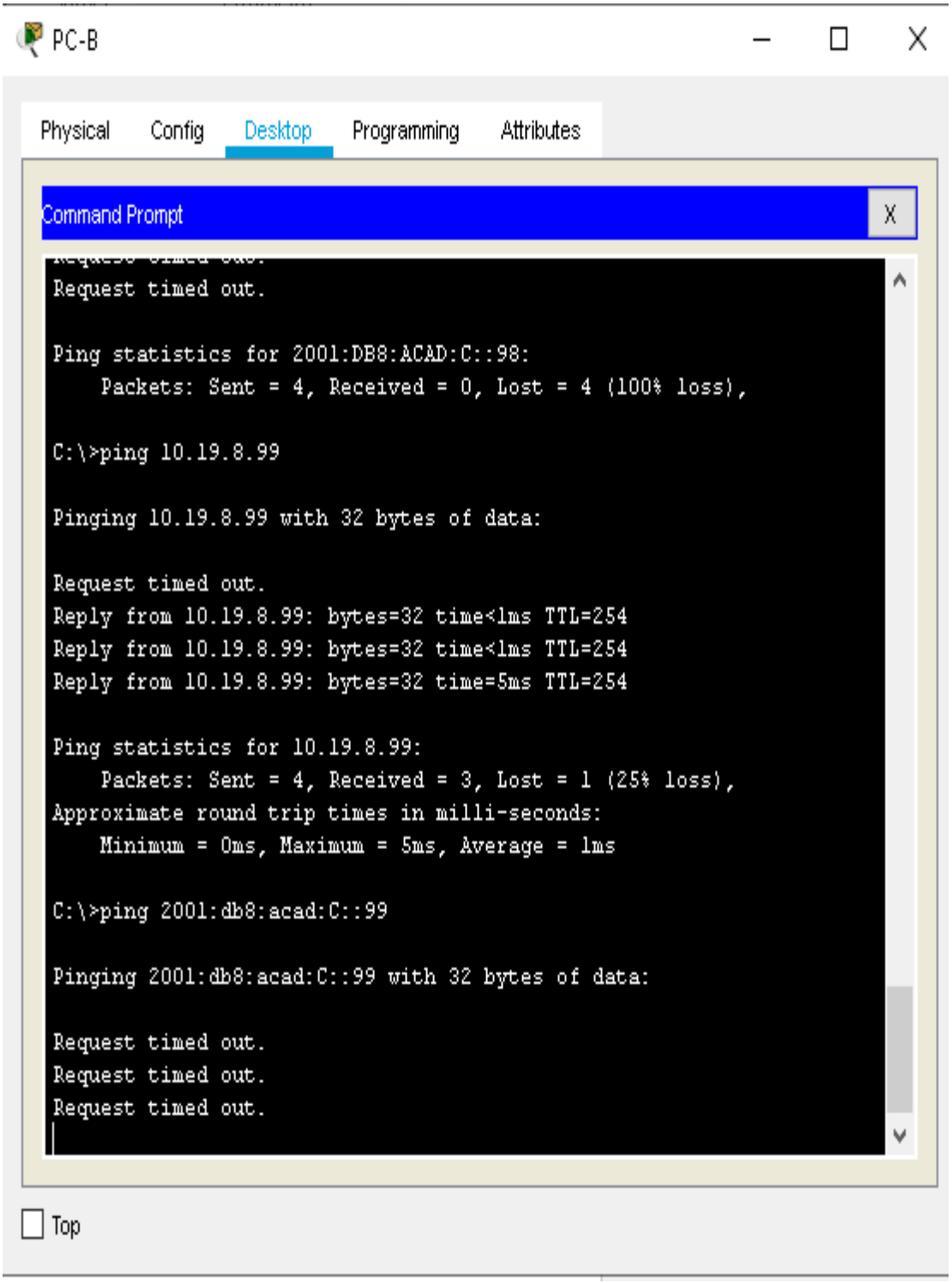


Figura 27. ping de PC-B a S1 VLAN 4_IPv6_FALLA

2. ESCENARIO 2

Descripción general

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

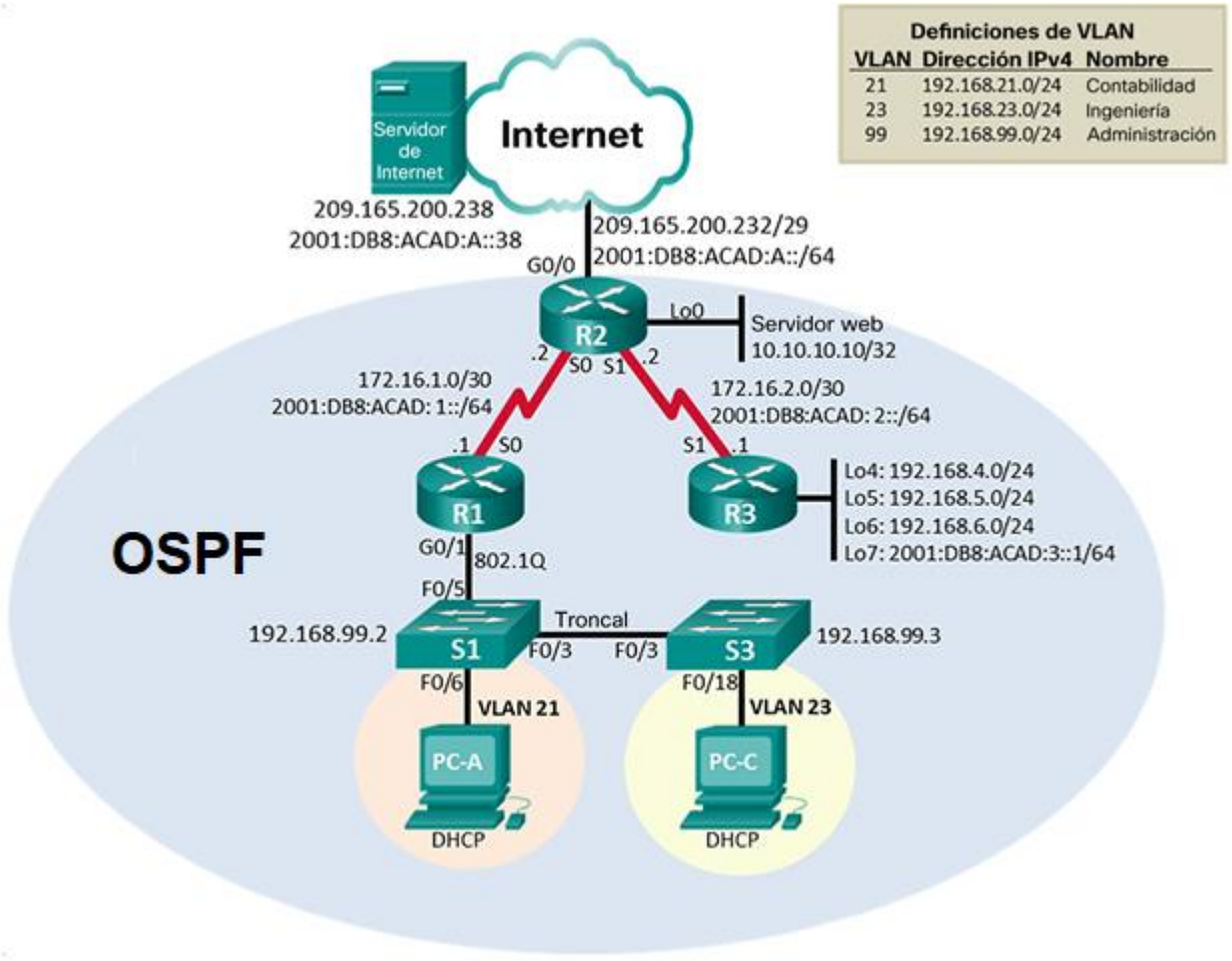


Figura 28. Topología 2

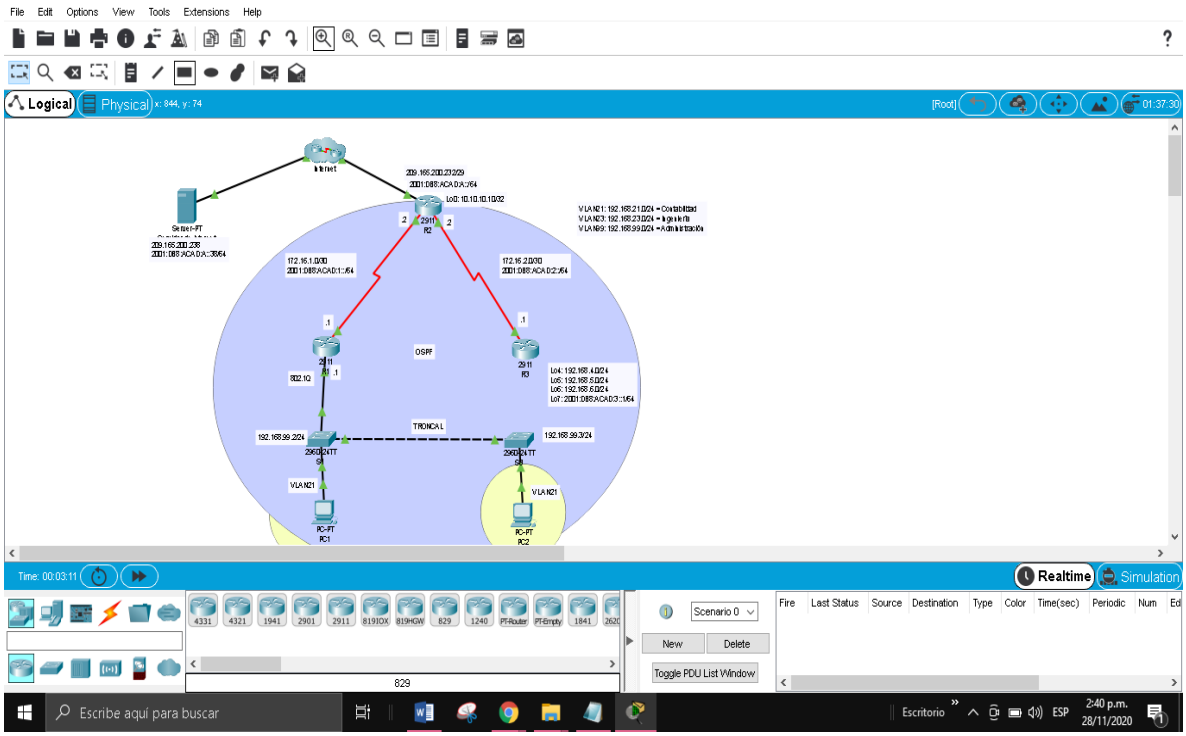


Figura 29. Topología 2 montada en simulador Packet Tracer

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.

En cada tabla en la columna comando **IOS** o **especicación,** se adjunta los comandos usados para así cumplir a cabalidad con los requerimientos planteados en cada parte y sus respectivos pasos.

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	#delete flash:config.text

de todos los switches y eliminar la base de datos de VLAN anterior	#delete flash: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 11. Tabla de configuraciones básicas realizadas_Paso 1_Parte 1

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):

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Tabla 12. Tabla de elementos a configurar y su especificación_Paso 1_Parte 2

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:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Enable Configure terminal no ip domain-lookup

Elemento o tarea de configuración	**Especificación**
Nombre del router R1	Enable Configure terminal Hostname R1
Contraseña de exec privilegiado cifrada class	Enable Configure terminal Enable secret class
Contraseña de acceso a la consola con clave cisco	Enable Configure terminal Line console 0 Password cisco login
Contraseña de acceso Telnet con password cisco	Enable Configure terminal Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Enable Configure terminal service password-encryption
Mensaje MOTD - Se prohíbe el acceso no autorizado.	Enable Configure terminal Banner motd & Se prohibe el acceso no autorizado &
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	Enable Configure terminal Interface serial 0/0/0 description CONEXION_CON_R2 ip address 172.16.1.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::1/64 ipv6 enable clock rate 128000 no shutdown

Elemento o tarea de configuración	Especificación
Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	Enable Configure terminal ip route 0.0.0.0 0.0.0.0 Serial0/0/0 ipv6 route ::/0 Serial0/0/0

Tabla 13. Tabla de configuraciones realizadas en R1_Paso 2_Parte 2

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Enable Configure terminal no ip domain-lookup
Nombre del router R2	Enable Configure terminal Hostname R2
Contraseña de exec privilegiado cifrada class	Enable Configure terminal Enable secret class
Contraseña de acceso a la consola con clave cisco	Enable Configure terminal Line console 0 Password cisco login
Contraseña de acceso Telnet con password cisco	Enable Configure terminal Line vty 0 4 Password cisco login

Cifrar las contraseñas de texto no cifrado	Enable Configure terminal service password-encryption
Habilitar el servidor HTTP	ip http server (Este commando solo funciona en un router real, en packet tracer no se puede)
Mensaje MOTD - Se prohíbe el acceso no autorizado	Enable Configure terminal Banner motd & Se prohibe el acceso no autorizado &
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	Enable Configure terminal interface Serial0/0/0 description Conexion_con_R1 ip address 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::2/64 ipv6 enable no shutdown
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	Enable Configure terminal interface Serial0/0/1 description CONEXION_CON_R3 ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::2/64 ipv6 enable ipv6 ospf 1 area 0 clock rate 128000 no shutdown

Interfaz G0/0 (simulación de Internet) Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	interface GigabitEthernet0/0 description INTERNET ip address 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64 ipv6 enable no shutdown
Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	Enable Configure terminal interface Loopback0 ip address 10.10.10.10 255.255.255.255
Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	Enable Configure terminal ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 ipv6 route ::/0 GigabitEthernet0/0

Tabla 14.Tabla de configuraciones realizadas en R2_Paso 3_Parte 2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Enable Configure terminal no ip domain-lookup
Nombre del router R3	Enable Configure terminal Hostname R3
Contraseña de exec privilegiado cifrada class	Enable Configure terminal Enable secret class

Contraseña de acceso a la consola con clave cisco	Enable Configure terminal Line console 0 Password cisco login
Contraseña de acceso Telnet con clave cisco	Enable Configure terminal Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Enable Configure terminal Service password-encryption
Mensaje MOTD - Se prohíbe el acceso no autorizado	Enable Configure terminal Banner motd & Se prohibe el acceso no autorizado &
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	Enable Configure terminal interface Serial0/0/1 description CONEXION_CON_R2 ip address 172.16.2.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::1/64 ipv6 enable
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	Enable Configure terminal interface Loopback4 ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	Enable Configure terminal interface Loopback5 ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	Enable Configure terminal interface Loopback6 ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	Enable Configure terminal interface Loopback7 ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	Enable Configure terminal ip route 0.0.0.0 0.0.0.0 Serial0/0/1 ipv6 route ::/0 Serial0/0/1

Tabla 15.Tabla de configuraciones realizadas en R3_Paso 4_Parte 2

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Enable Configure terminal no ip domain-lookup
Nombre del switch S1	Enable Configure terminal Hostname S1
Contraseña de exec privilegiado cifrada class	Enable Configure terminal Enable secret class
Contraseña de acceso a la consola con clave cisco	Enable Configure terminal Line console 0 Password cisco login

Contraseña de acceso Telnet con clave cisco	Enable Configure terminal Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Enable Configure terminal service password-encryption
Mensaje MOTD - Se prohíbe el acceso no autorizado	Enable Configure terminal Banner motd & Se prohibe el acceso no autorizado &

Tabla 16. Tabla de configuraciones realizadas en S1_Paso 5_Parte 2

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Enable Configure terminal no ip domain-lookup
Nombre del switch	Enable Configure terminal Hostname S3
Contraseña de exec privilegiado cifrada class	Enable Configure terminal Enable secret class
Contraseña de acceso a la consola con clave cisco	Enable Configure terminal Line console 0 Password cisco login

Contraseña de acceso Telnet con clave cisco	Enable Configure terminal Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Enable Configure terminal service password-encryption
Mensaje MOTD	Enable Configure terminal Banner motd & Se prohibe el acceso no autorizado &

Tabla 17. Tabla de configuraciones realizadas en S3_Paso 6_Parte 2

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:

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	209.165.200.225	Falló por que no pertenece al segmento y se tuvo que modificar por la ip 209.165.200.238 que es la que se indica en la topología y no en el requerimiento de configuración.

Tabla 18. Tabla de configuraciones realizadas en paso 7_Parte 2_Vericación de conectividad

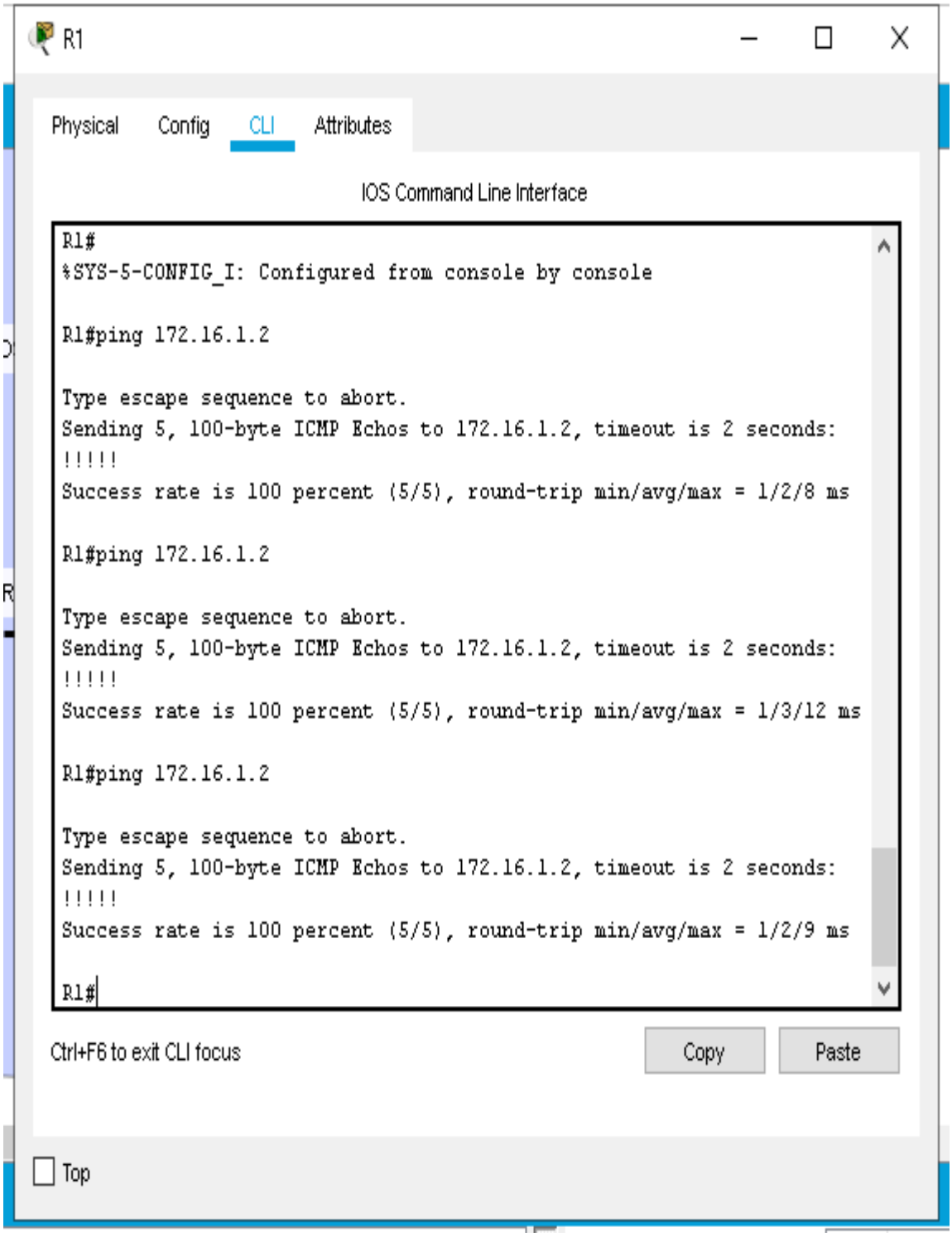


Figura 30. ping de R1 a R2_172.16.1.2_OK

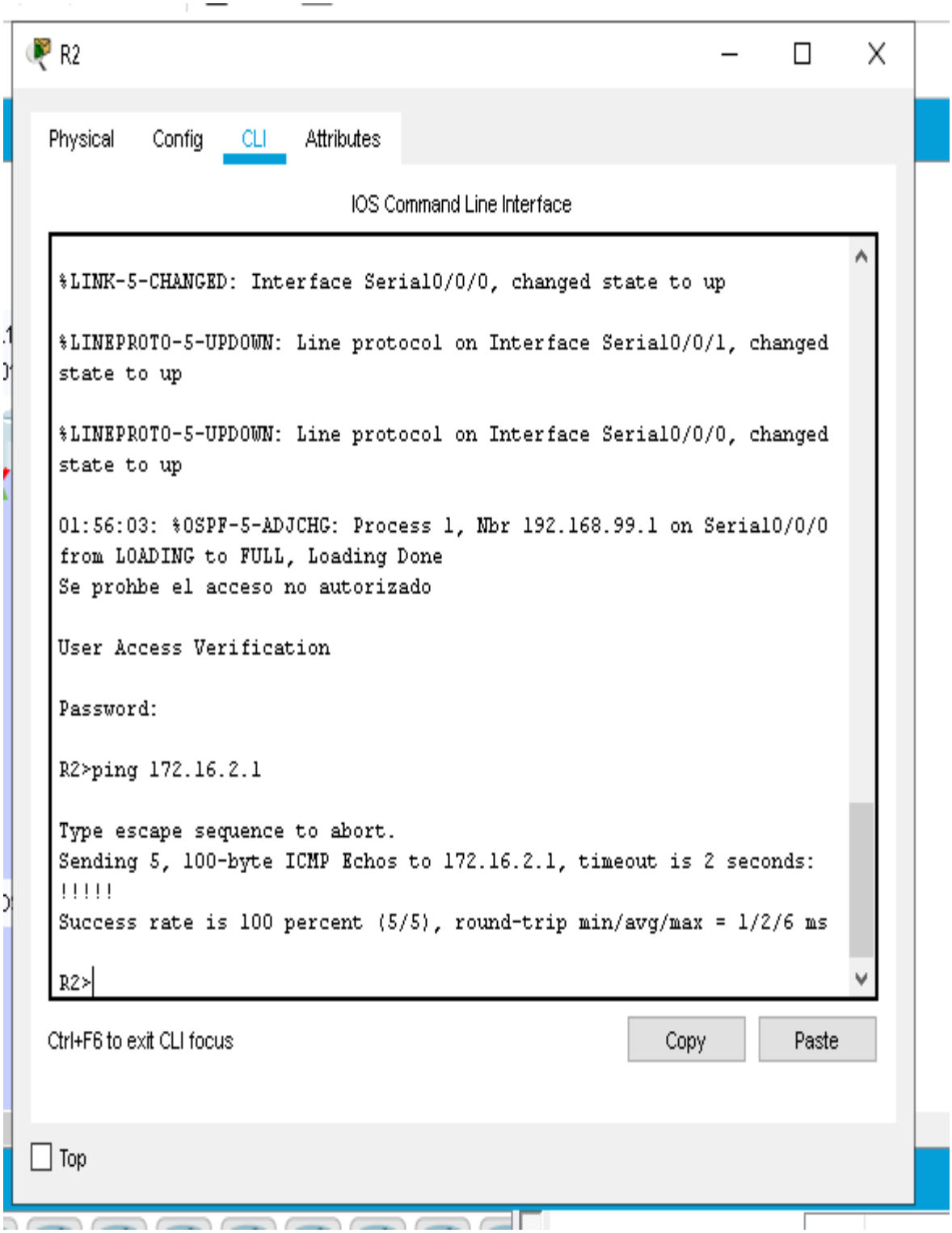


Figura 31. ping de R2 a R1_172.16.2.1_OK

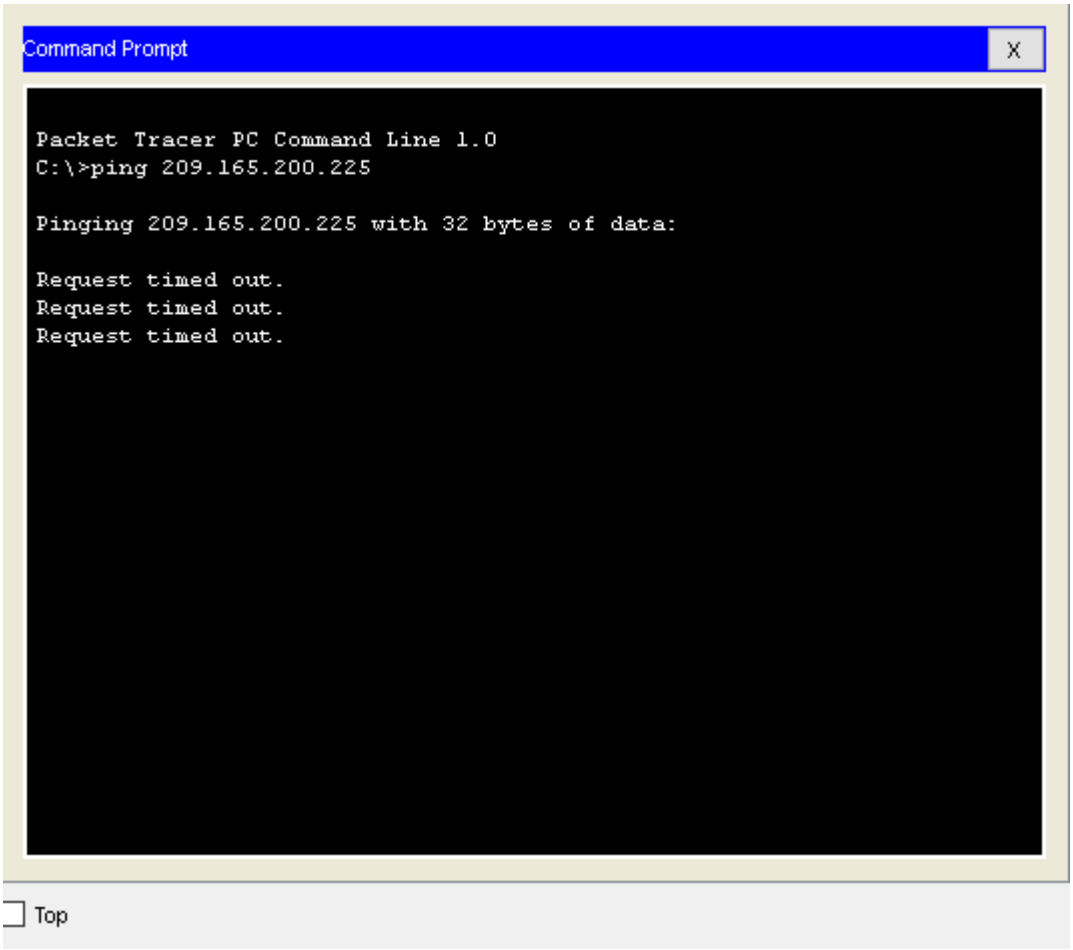


Figura 32. ping de PC de internet a Gateway predeterminado 209.165.200.225 _FALLA

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

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:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	Enable Configure terminal Vlan 21 Exit Vlan 23 Exit Vlan 99
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	Enable Configure terminal interface Vlan99 ip address 192.168.99.2 255.255.255.0 no shutdown
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	Enable Configure terminal ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	Enable Configure terminal interface FastEthernet0/3 switchport mode trunk switcport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	Enable Configure terminal interface FastEthernet0/5 switchport mode trunk switcport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	Enable Configure terminal Interface range FastEthernet 0/1 – 2 switchport mode access Interface FastEthernet 0/4 switchport mode access Interface range FastEthernet 0/6 – 24 switchport mode access
Asignar F0/6 a la VLAN 21	Enable Configure terminal Interface FastEthernet 0/6 switchport mode access Switchport access vlan 21
Apagar todos los puertos sin usar	Enable Configure terminal Interface range FastEthernet 0/1 – 2 shutdown Interface FastEthernet 0/4 shutdown Interface range FastEthernet 0/7 – 24 shutdown

Tabla 19. Tabla de configuraciones realizadas en S1_Paso 1_Parte 3

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	Enable Configure terminal Vlan 21 Exit Vlan 23 Exit Vlan 99
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	Enable Configure terminal interface Vlan99 ip address 192.168.99.3 255.255.255.0 no shutdown
Asignar el gateway predeterminado. Asignar la primera dirección IP en la subred como gateway predeterminado.	Enable Configure terminal ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	Enable Configure terminal interface FastEthernet0/3 switchport mode trunk switcport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	Enable Configure terminal Interface range FastEthernet 0/1 – 2 switchport mode access Interface range FastEthernet 0/4 – 24 switchport mode access

Asignar F0/18 a la VLAN 21	Enable Configure terminal Interface FastEthernet 0/18 switchport mode access Switchport access vlan 21
Apagar todos los puertos sin usar	Enable Configure terminal Interface range FastEthernet 0/1 – 2 shutdown Interface range FastEthernet 0/4 – 17 Shutdown Interface range FastEthernet 0/19 – 24 shutdown

Tabla 20. Tabla de configuraciones realizadas en S3_Paso 2_Parte 3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	Enable Configure terminal interface GigabitEthernet0/1.21 description CONTABILIDAD encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	Enable Configure terminal interface GigabitEthernet0/1.23 description INGENIERIA encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	Enable Configure terminal interface GigabitEthernet0/1.99 description ADMINISTRACION encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1 No shutdown	Enable Configure terminal interface GigabitEthernet0/1 no shutdown

Tabla 21. Tabla de configuraciones realizadas en R1_Paso 3_Parte 3

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:

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

Tabla 22. Tabla de verificación de conectividad R1

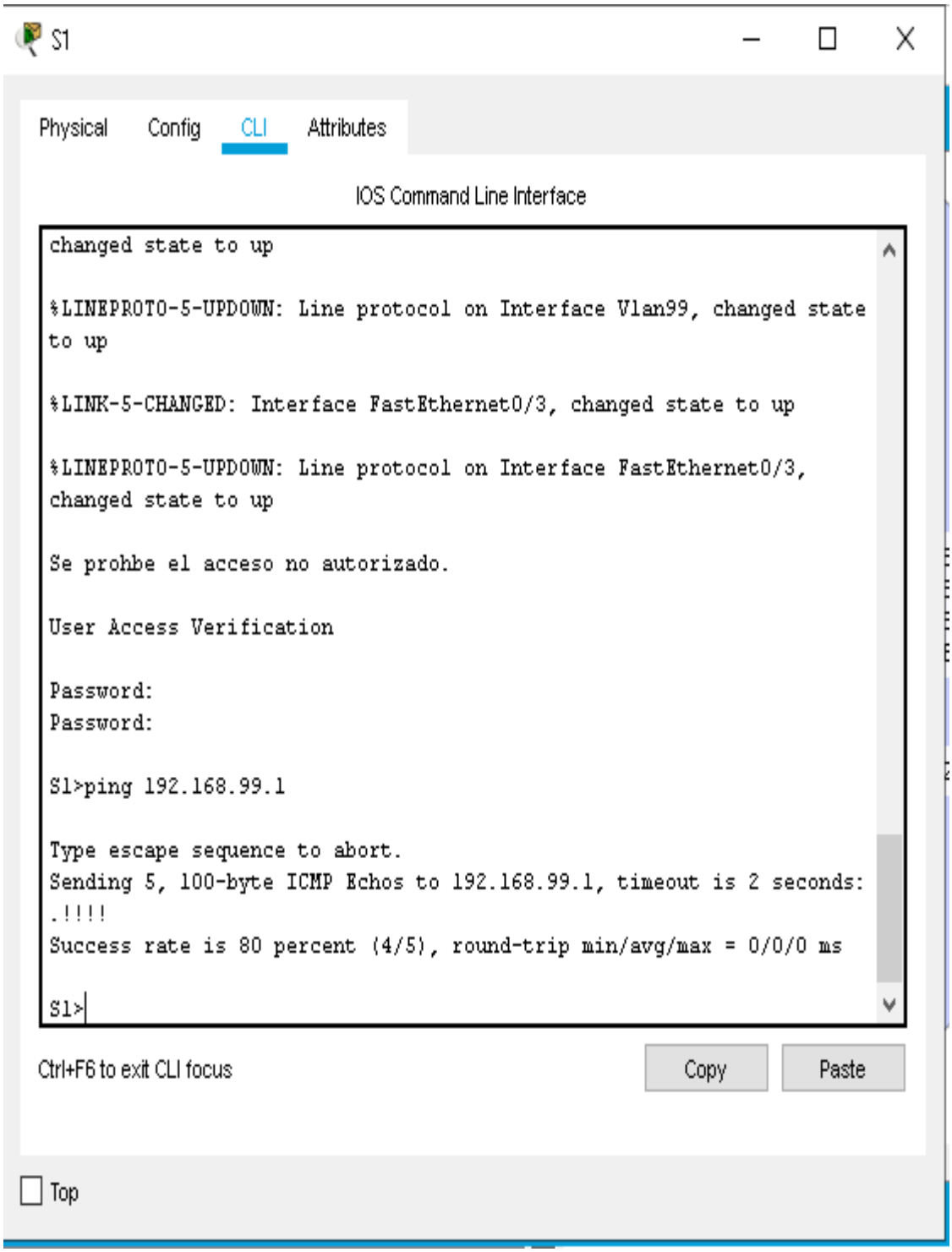


Figura 33. ping de S1 a dirección VLAN 99_ 192.168.99.1_OK

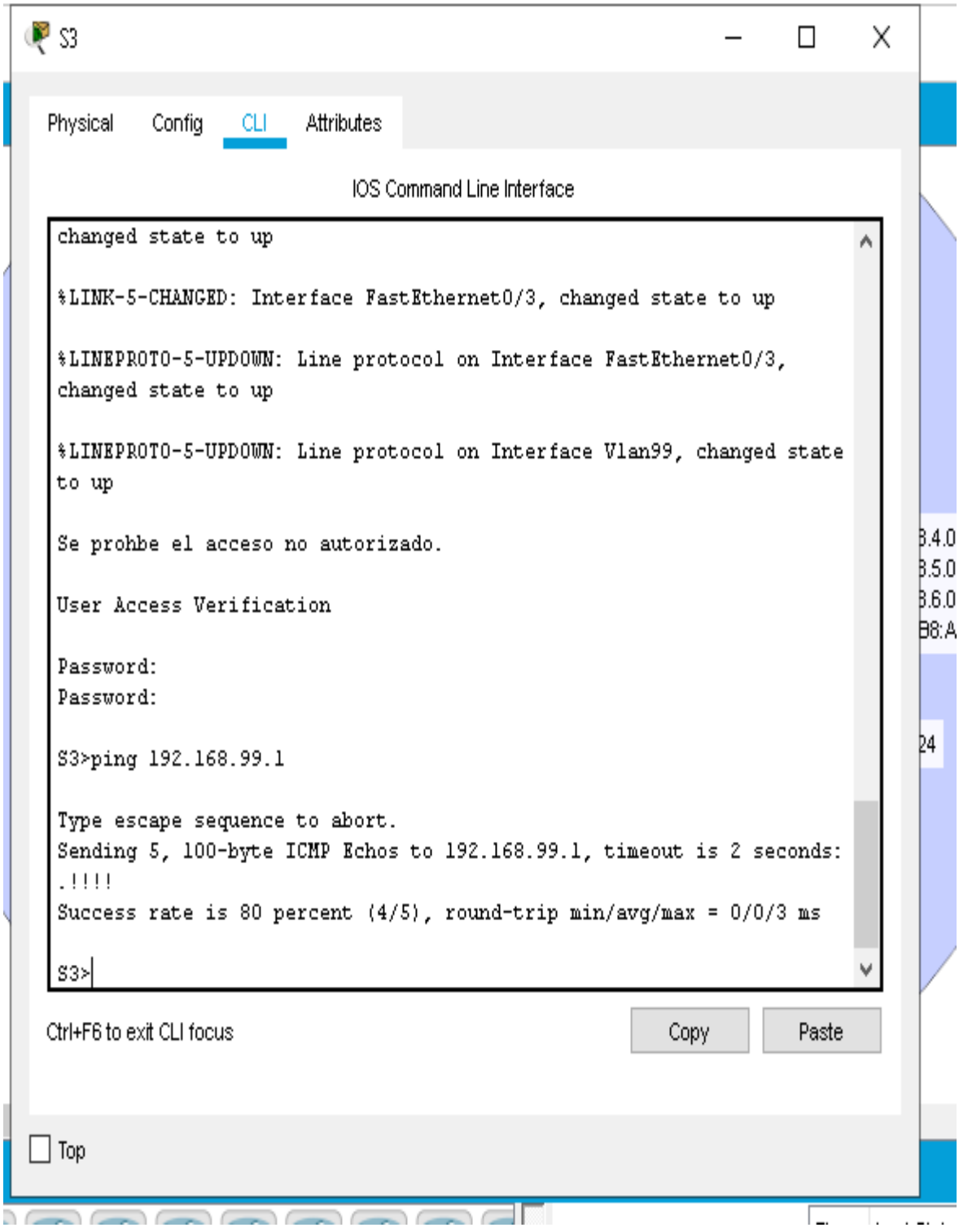


Figura 34. ping de S3 a dirección VLAN 99_ 192.168.99.1_OK

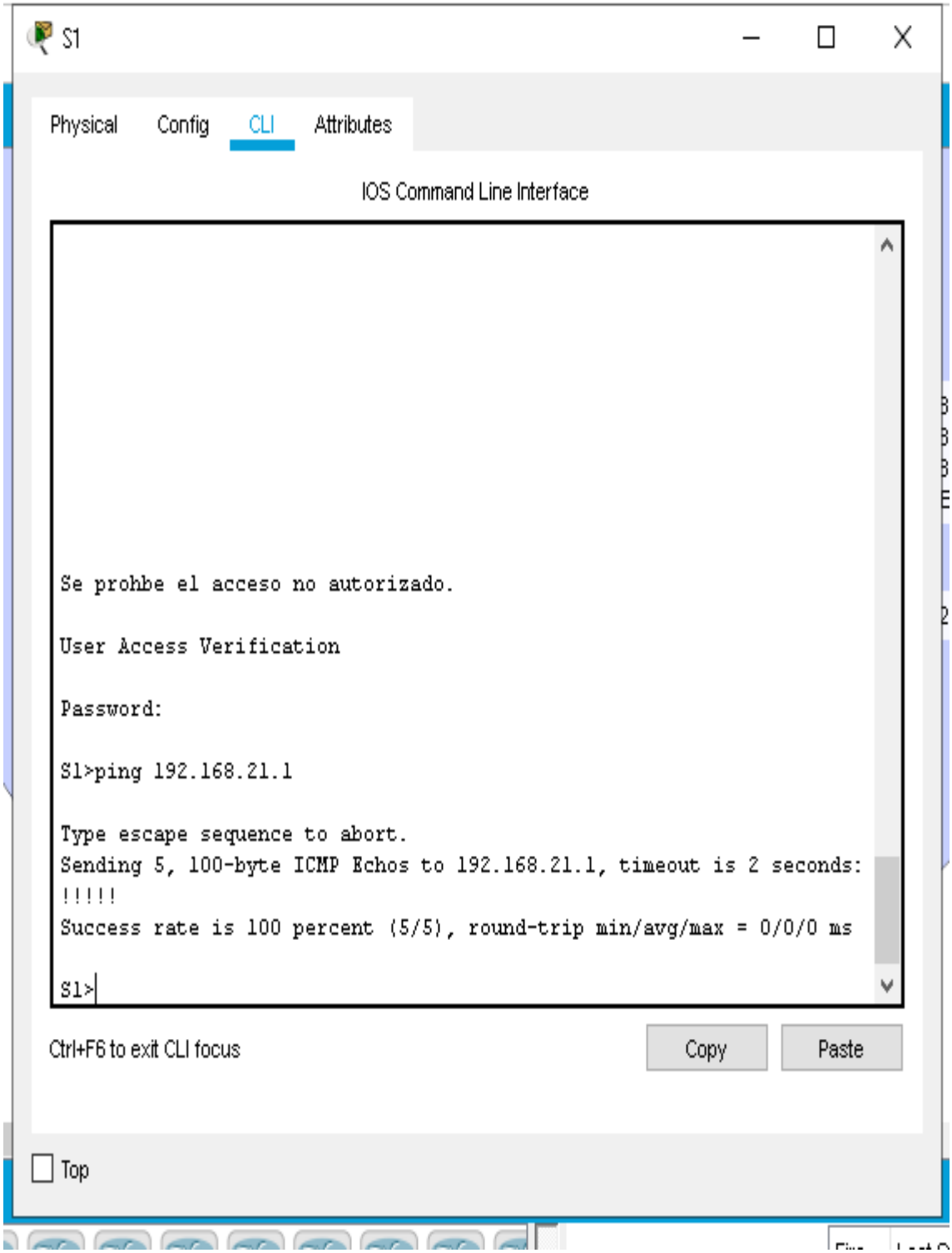


Figura 35. ping de S1 a dirección VLAN 21_ 192.168.21.1_OK

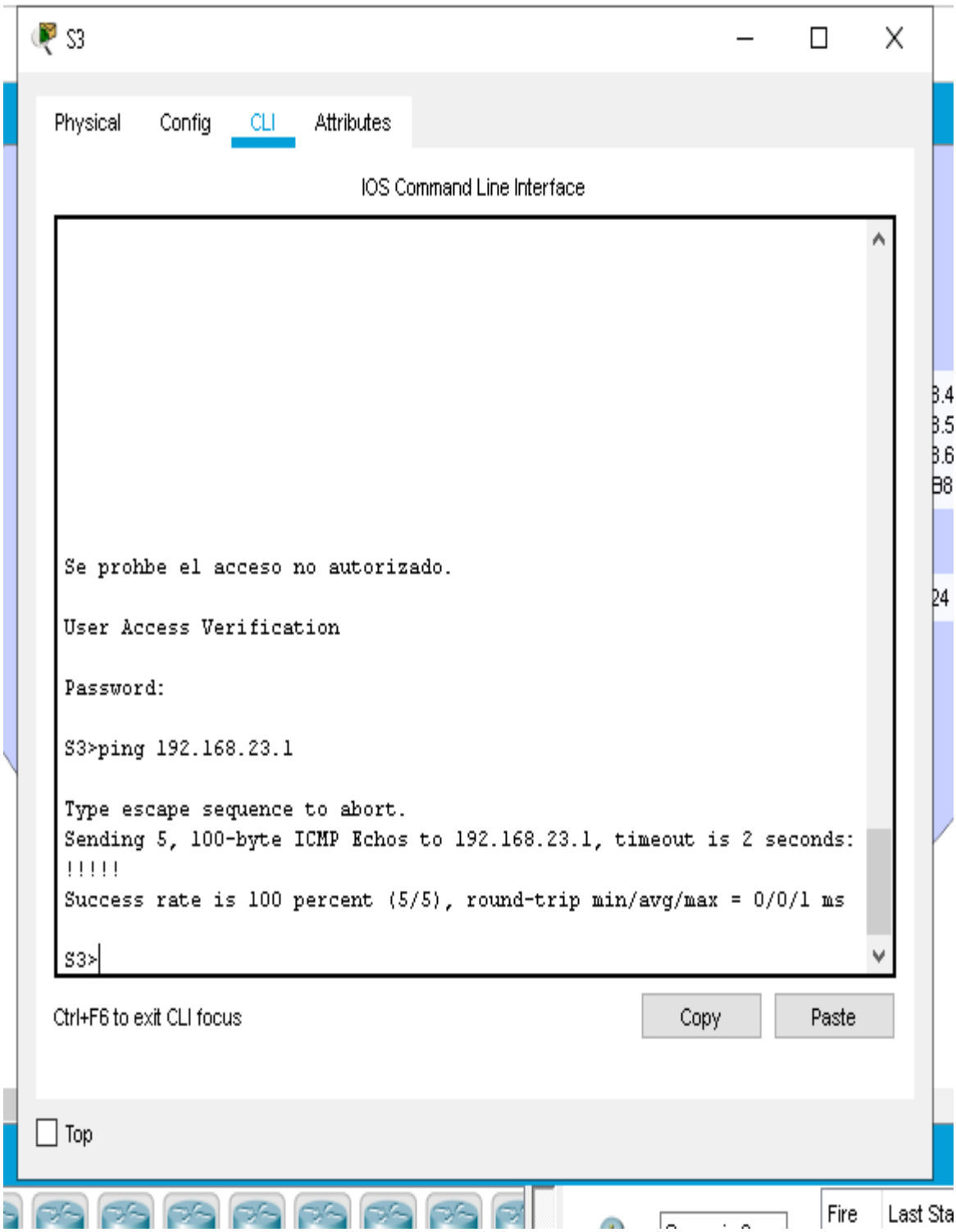


Figura 36. ping de S3 a dirección VLAN 23_ 192.168.23.1_OK

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:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Enable Configure terminal router ospf 1 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 network 172.16.1.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	Enable Configure terminal router ospf 1 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 network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	Enable Configure terminal router ospf 1 passive-interface GigabitEthernet0/1 passive-interface GigabitEthernet0/1.21 passive-interface GigabitEthernet0/1.23 passive-interface GigabitEthernet0/1.99
Desactive la sumarización automática	Esto no aplica en OSPF en RIP o EIGRP si, así que en este caso lo que se puede hacer es una sumarización manual para OSPF, más no desactivar una sumarización automática por que esto no existe en este protocolo.

Tabla 23. Tabla de configuraciones realizadas en R1_Paso 1_Parte 4

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Enable Configure terminal router ospf 1 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	Enable Configure terminal router ospf 1 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	Enable Configure terminal router ospf 1 passive-interface Loopback0
Desactive la sumarización automática.	Esto no aplica en OSPF en RIP o EIGRP si, así que en este caso lo que se puede hacer es una sumarización manual para OSPF, más no desactivar una sumarización automática por que esto no existe en este protocolo.

Tabla 24. Tabla de configuraciones realizadas en R2_Paso 2_Parte 4

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Enable Configure terminal ipv6 router ospf 1 router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	Enable Configure terminal interface Serial0/0/0 ipv6 ospf 1 area 0 interface Serial0/0/1 ipv6 ospf 1 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Enable Configure terminal Router ospf 1 passive-interface Loopback0
Desactive la sumarización automática.	Esto no aplica en OSPF en RIP o EIGRP si, así que en este caso lo que se puede hacer es una sumarización manual para OSPF, más no desactivar una sumarización automática por que esto no existe en este protocolo.

Tabla 25. Tabla de configuraciones realizadas en R2_Paso 3_Parte 4

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:

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?	Enable Show ip ospf database show ip route show run
¿Qué comando muestra solo las rutas OSPF?	Show ip ospf neighbor
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | section router ospf

Tabla 26. Paso 15: Verificación de información OSPF

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:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
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.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Tabla 27. Tabla de configuraciones realizadas en R1_Paso 1_Parte 5

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	No es posible debido a que esto solo se puede habilitar en equipos reales o emulados con un IOS o Sistema operative real de cisco. Packet tracer no soporta esta configuración.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No es posible debido a que esto solo se puede habilitar en equipos reales o emulados con un IOS o Sistema operative real de cisco. Packet tracer no soporta esta configuración.

Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.229**	ip nat inside source static 209.165.200.238 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	Enable Configure terminal interface GigabitEthernet0/0 ip nat inside interface Serial0/0/0 ip nat outside interface Serial0/0/1 ip nat outside
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	Aqui se debe configurar R2 según el paso pero en el enunciado pide hacerlo en R1 y R3 R1 Enable Configure terminal access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 R3 Enable Configure terminal access-list 1 permit 192.168.4.0 0.0.0.255 access-list 1 permit 192.168.5.0 0.0.0.255 access-list 1 permit 192.168.6.0 0.0.0.255

Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228**	R1 Enable Configure terminal ip nat pool INTERNET 209.165.200.225 209.165.200.226 netmask 255.255.255.252 R3 Enable Configure terminal ip nat pool INTERNET 209.165.200.227 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R1: ip nat inside source list 1 pool INTERNET R3: ip nat inside source list 1 pool INTERNET

Tabla 28. Tabla de configuraciones realizadas en R2_Paso 2_Parte 5

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.

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**	Se visualiza el servidor pero no pide credenciales debido a que lo que se solicitó es para un entorno real, en packet tracer no se podría habilitar http en el router, debido a que se está habilitando el servidor de internet como servidor http y al estar publicando mediante nat estatico dicho servidor para qu elas pcs puedan acceder a el, no obstante las credenciales no sirven ya que estas están configuradas en el router y no en el servidor de internet.

Tabla 29. Paso 8: Verificación protocolo DHCP y la NAT estática

Parte 6: Configurar NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	Enable clock set 09:00:30 MAR 5 2016
Configure R2 como un maestro NTP. Nivel de estrato: **5**	Enable Configure terminal ntp master 5
Configurar R1 como un cliente NTP. Servidor: **R2**	Enable Configure terminal ntp server 172.16.1.2 ntp update-calendar
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Enable Configure terminal ntp server 172.16.2.2 Ntp update-calendar
Verifique la configuración de NTP en R1.	Enable Show running-config

Tabla 30. Configuración NTP

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

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

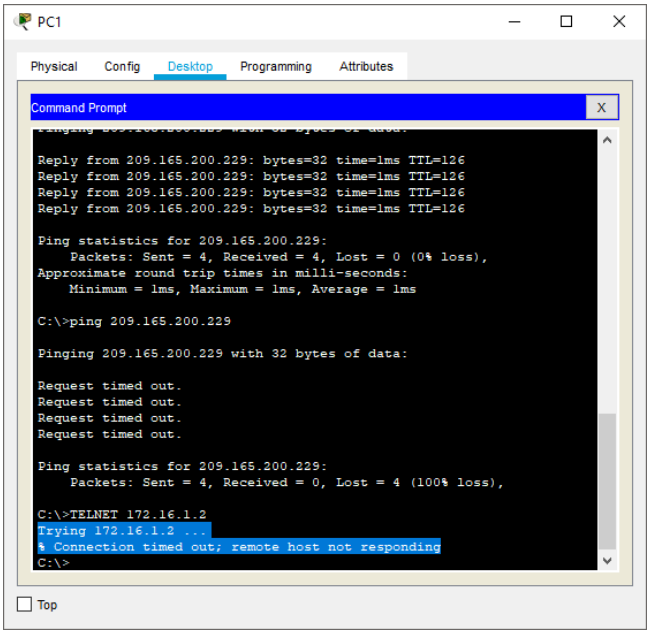
Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: **ADMIN-MGT**	Enable Configure terminal ip access-list standard ADMIN-MGT permit 172.16.1.0 0.0.0.3
Aplicar la ACL con nombre a las líneas VTY	Enable Configure terminal Line vty 0 4 Access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	Enable Configure terminal Line vty 0 4 transport input telnet
Verificar que la ACL funcione como se espera	Funciona correctamente!!. Entrando al Command Pront de PC1 pruebo hacienda telnet al router R2 y no se establece la conexión tal y como se pide. 

Tabla 31. Configuración de restricción de acceso a las líneas VTY en el R2

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

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

Tabla 32. configuración comando de CLI

CONCLUSIONES

Con el desarrollo del presente proyecto se plantea una gran inclinación personal al ámbito de configuración de redes de conmutación, podría tomarse como un enfoque al ámbito de la especialidad de dicha área teniendo en cuenta que está en el auge de la tecnología y seguirá cogiendo fuerza por la gran necesidad en el día a día personal y empresarial.

CCNA (Cisco Certified Network Associate), dota de grandes conocimientos en redes WAN/LAN, nos provee de destreza y habilidades necesarias para diseñar, implementar y realizar el respectivo mantenimiento a estructuras de redes integrales.

Por medio del protocolo DCHP, realizamos configuración dinámica de host mediante un protocolo de red de tipo cliente/servidor, siendo este un servidor DHCP de gran utilidad conocido por su función de asignar dinámicamente una dirección IP

La herramienta de simulación exclusiva de Cisco Systems, Packet Tracer en ocasiones limita al uso de algunos protocolos debido a los limitantes de configuraciones de procesos que tienen funcionalidad solo con herramientas de dicho fabricante.

BIBLIOGRAFÍA

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

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

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

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

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

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

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

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

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

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

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

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

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

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

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

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

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

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

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

ANEXOS

ANEXO 1

Enlace de descarga de archivos de simulación

https://drive.google.com/drive/folders/1mYEQEdMvr2jAPtsFewzW0bknzlzaRYzH?usp=sharing

ANEXO 2

Artículo Científico IEEE

https://drive.google.com/drive/folders/1MZQbT2V9a15lCo4oeoi77QV9H92EtZ1J?usp=sharing