DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JUAN DAVID ROMERO MORA

Diplomado de opción de grado presentado para optar el título de

INGENIERO ELECTRONICO

TUTOR:

HECTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERIA ELECTRONICA

BOGOTÁ D.C.

2021

NOTAS DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

Bogotá, 16 de Julio de 2021

CONTENIDO

INTRODUCCIÓN

En el presente trabajo se utiliza herramientas de simulación con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento sobre un escenario en el que se propone una pequeña red LAN en el cual se debe realizar 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.

En el 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.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

- ***CISCO:*** empresa de tecnología estadounidense que opera en todo el mundo y que es conocida por sus productos de redes informáticas y de telecomunicaciones.

- ***LAN:*** o conocida también como red de área local, es una red de dispositivos host, de conmutación, de ruteo, entre otros los cuales abarcan una area relativamente reducida como una casa, apartamento, edificio.

- ***SWITCH:*** dispositivo que conecta varios dispositivos como computadoras, puntos de acceso inalámbricos, servidores, impresoras entre otros a la misma res.

- ***ROUTER:*** dispositivo que permite interconectar computadoras que funcionan en una red. Por medio de un router, las redes se hacen mas eficientes al mejorar el rendimiento y disminuir el tiempo de entrega de paquetes entre redes, determinando las mejores rutas para ello.

- ***CISCO IOS:*** es el software utilizado en la gran mayoría de routers y switches de Cisco Systems. Es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra con un sistema operativo multitarea.

RESUMEN

En este documento se desarrollan dos escenarios propuestos enfocados en el desarrollo de redes LAN/WAN así como configuración de dispositivos CISCO tales como router, switches y dispositivos host como computadoras y servidores. Todo lo anterior encaminado a profundizar sobre los conceptos básicos de redes como conmutación, enrutamiento, protocolo TCP/IP, IPv4 y IPv6, protocolo de configuración dinámica de host o DHCP, direccionamiento IP, entre otros.

De esta forma se dará cumplido con el trabajo final del Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas Lan / Wan).

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

ABSTRACT

This document develops two proposed scenarios focused on the development of LAN / WAN networks as well as the configuration of CISCO devices such as routers, switches and host devices such as computers and servers. All of the above aimed at delving into the basic concepts of networks such as switching, routing, TCP / IP protocol, IPv4 and IPv6, dynamic host configuration protocol or DHCP, IP addressing, among others.

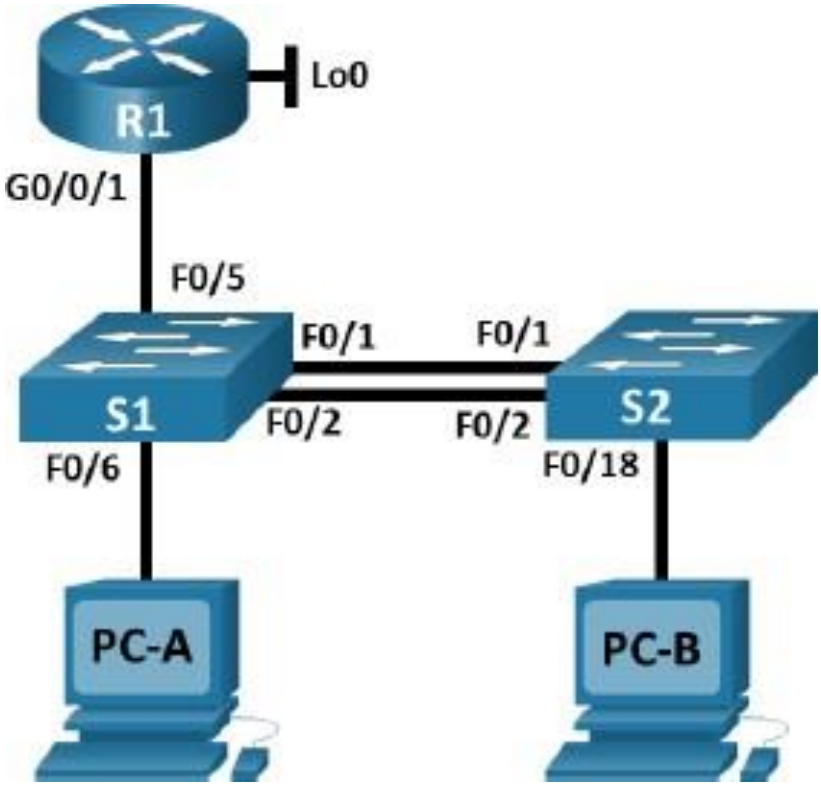
In this way, the final work of the Cisco Deepening Diploma (Design and Implementation of Integrated Solutions Lan / Wan) will be completed.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

ESCENARIO 1

Topología

Figura 1: Topología de red



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

Tabla 1: Tabla de VLan

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

Tabla 2 Tabla de direccionamiento

Tabla de asignación de direcciones Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
R1 G0/0/1.2	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
R1 G0/0/1.3	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
R1 G0/0/1.4	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
VLAN S1 4	2001:db5:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
S2 VLAN 4	2001:db5:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db5:acad:b: :50 /64	fe80::1

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

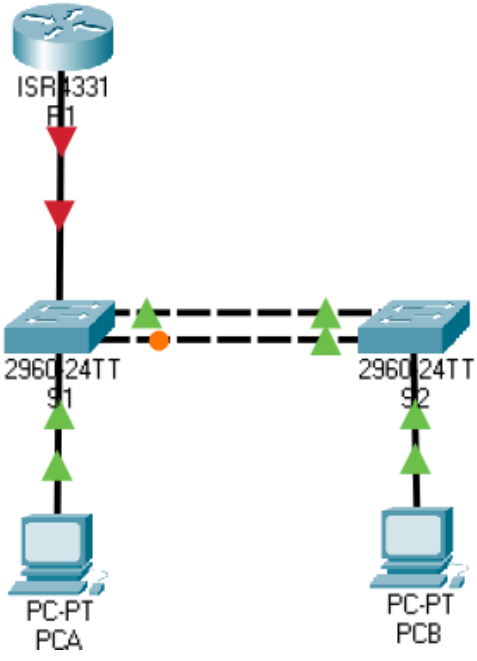
INSTRUCCIONES

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

Paso 1: Inicializar y volver a cargar el router y el switch

Inicialmente se procede a colocar los dispositivos correspondientes en la herramienta packet tracer y a realizar las respectivas conexiones entre los mismos.

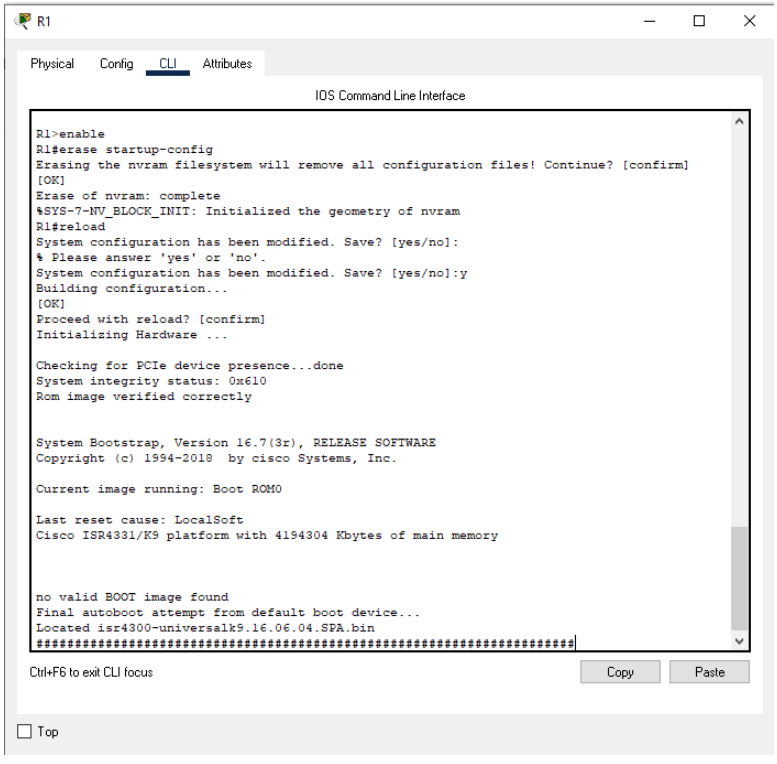
Figura 2: Topología en packet tracer



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

    - **Proceso en R1**

Figura 3: Borrado de configuraciones de inicio y reinicio del Router R1



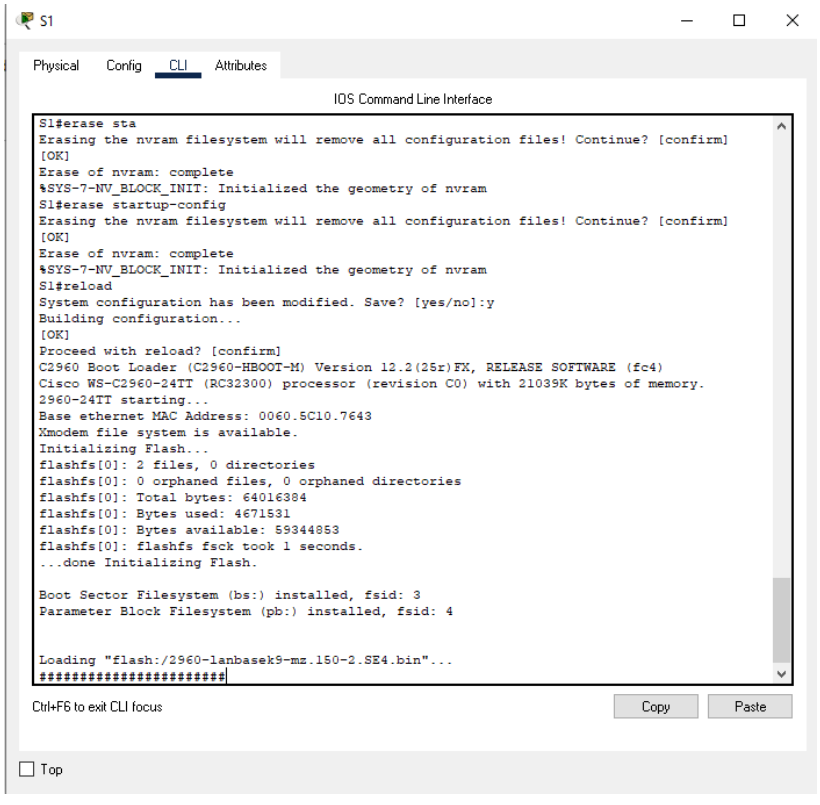
Comandos ejecutados:

Tabla 3: Comandos inicialización R1

COMANDO	DESCRIPCIÓN
R1>enable	Cambio a modo EXEC privilegiado
R1#erase startup-config	Se elimina la configuración de inicio
R1#reload	Se reinicia el dispositivo

- **Proceso en S1**

Figura 4: Borrado de configuraciones de inicio y reinicio del Switch S1

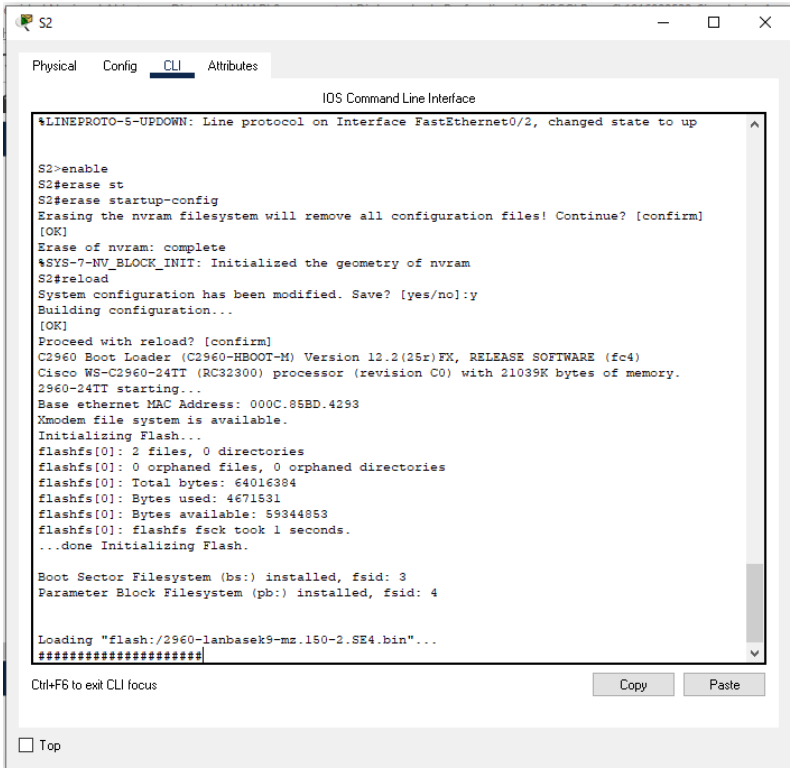


Comandos ejecutados:

COMANDO	DESCRIPCIÓN
S1>enable	Cambio a modo EXEC privilegiado
S1#erase startup-config	Se elimina la configuración de inicio
S1#reload	Se reinicia el dispositivo

- **Proceso en S2**

Figura 5: Borrado de configuraciones de inicio y reinicio del Switch S2



Comandos ejecutados:

COMANDO	DESCRIPCIÓN
S1>enable	Cambio a modo EXEC privilegiado
S1#erase startup-config	Se elimina la configuración de inicio
S1#reload	Se reinicia el dispositivo

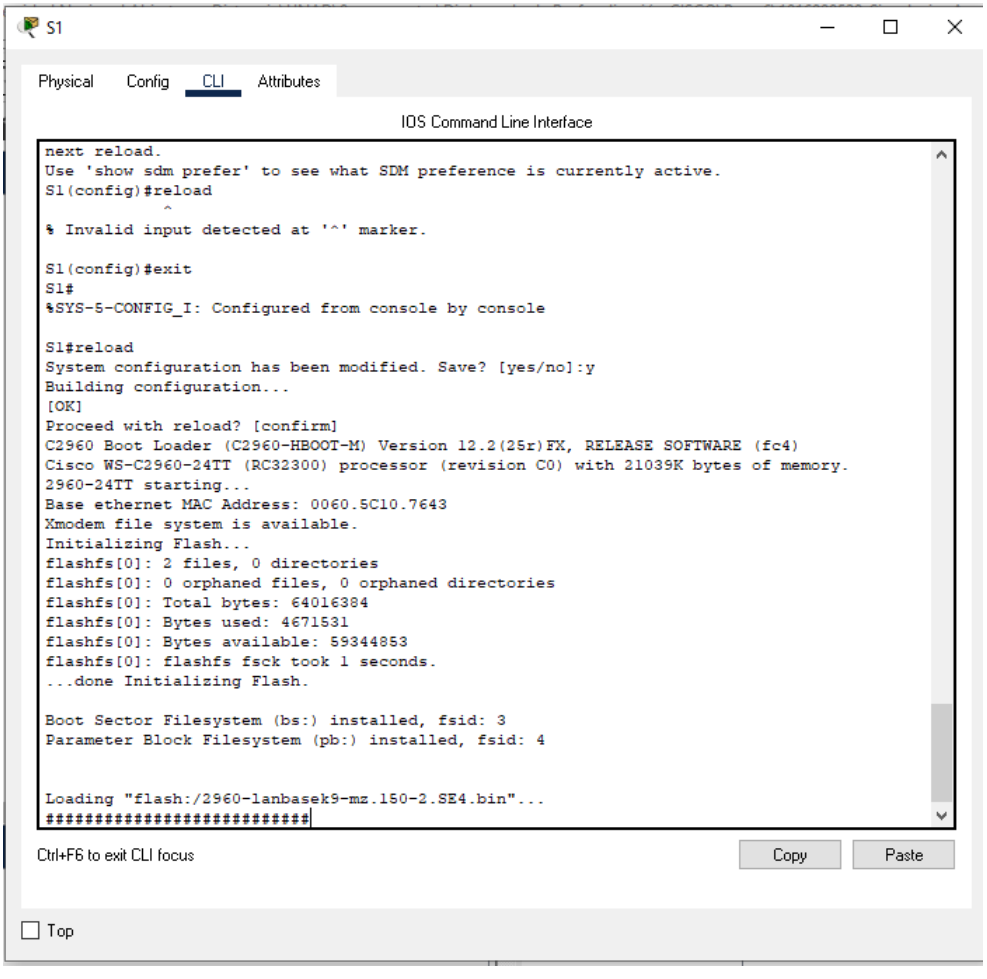
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Comandos ejecutados en S1:

Tabla 4: Comandos habilitación IPv6

COMANDO	DESCRIPCIÓN
S1>enable	Cambio a modo EXEC privilegiado
S1#configure terminal	Se accede al modo de configuración global
S1# sdm prefer dual-ipv4-and-ipv6 default	Se habilita el soporte IPv6
S1#reload	Se reinicia el dispositivo

Figura 6: Habilitación de IPv6 en S1

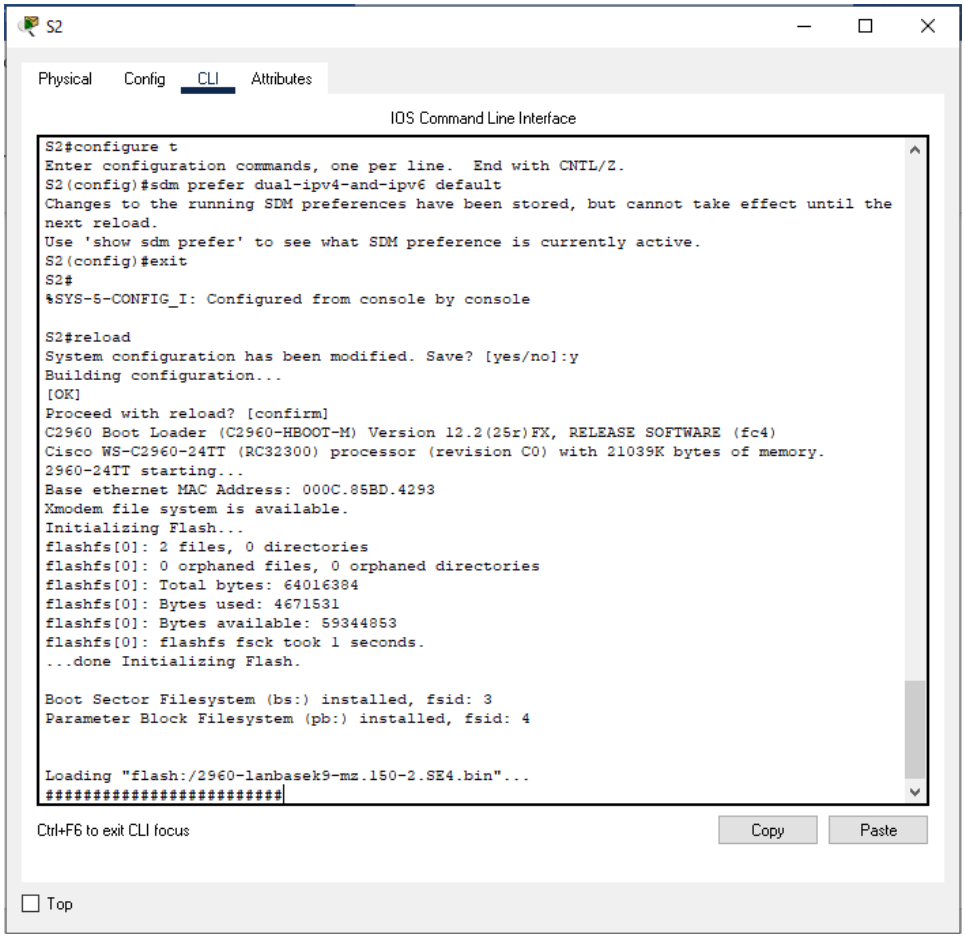


Comandos ejecutados en S2:

Tabla 5: Comandos habilitación IPv6

COMANDO	DESCRIPCIÓN
S2>enable	Cambio a modo EXEC privilegiado
S2#configure terminal	Se accede al modo de configuración global
S2# sdm prefer dual-ipv4-and-ipv6 default	Se habilita el soporte IPv6
S2#reload	Se reinicia el dispositivo

Figura 7: Habilitación de IPv6 en S2



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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6: Tareas de configuración para R1

Tarea	Especificación	Comando Ejecutado
Desactivar la búsqueda DNS		R1>enable R1#configure terminal R1(config)#no ip domain-lookup
Nombre del router	R1	R1(config)#hostname R1
Nombre de dominio	ccna-lab.com	R1(config #ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass	R1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	ciscoconpass	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	10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**	R1(config)#username admin privilege 15 secret admin1pass
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
Configurar VTY solo aceptando SSH		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 a este dispositivo esta prohibido#
Habilitar el routing IPv6		R1(config)#ipv6 unicast-routing
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.	R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN a VLAN2 Bikes R1(config-subif)#ip add 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#ipv6 add 2001:db5:acad:a::1/64 R1(config-subif)#no shutdown R1(config-subif)#exit

		R1(config)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description LAN a VLAN3 Trikes R1(config-subif)#ip add 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#ipv6 add 2001:db5:acad:b::1/64 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description LAN a VLAN4 Management R1(config-subif)#ip add 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#ipv6 add 2001:db5:acad:c::1/64 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description LAN a VLAN6 Native R1(config-subif)#no shutdown

		R1(config-subif)#exit
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**	R1(config)#interface lo0 R1(config-if)#description 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	Módulo de 1024 bits	R1(config)#crypto key generate rsa general-keys modulus 1024

Paso 3: Configure S1 y S2.

Las tareas de configuración en el S1 incluyen lo siguiente:

Tabla 7: Tareas de configuración para S1

Tarea	Especificación	Comando Ejecutado
Desactivar la búsqueda DNS.		S1>enable S1#config terminal S1(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda**	S1(config)#hostname S1
Nombre de dominio	**ccna-lab.com**	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass**	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	Nombre de usuario: **admin** Password: **admin1pass**	S1(config)#username admin privilege 15 secret admin1pass
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 a este dispositivo esta prohibido#
Generar una clave de cifrado RSA	**Módulo de 1024 bits**	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3	S1(config)#interface vlan 4

	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(config-if)#ip add 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db5: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	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config)#ip default-gateway 10.21.5.97

Las tareas de configuración en el S2 incluyen lo siguiente:

Tabla 8: Tareas de configuración para S2

Tarea	Especificación	Comando Ejecutado
Desactivar la búsqueda DNS.		S2>enable S2#config terminal S2(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda**	S2(config)#hostname S2
Nombre de dominio	**ccna-lab.com**	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass**	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	Nombre de usuario: **admin** Password: **admin1pass**	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)#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)#transport input ssh 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 a este dispositivo esta prohibido#
Generar una clave de cifrado RSA	**Módulo de 1024 bits**	S2(config)#crypto key generate rsa general-keys modulus 1024
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	S2(config)#interface vlan 4 S2(config-if)#ip add 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db5:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config)#ip default-gateway 10.21.5.97

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)
Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9: Tareas de configuración VLAN S1

Tarea	**Especificación**	**Comando Ejecutado**
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#interface fa0/1 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#interface fa0/2 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 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	Usar el protocolo LACP para la negociación	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 mode trunk S1(config)#switchport trunk native vlan 6 S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6	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	Permitir 3 direcciones MAC	S1(config)#interface fa0/6

en los puertos de acceso		S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#exit
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	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 Interfaces no utilizadas S1(config-if-range)#shutdown S1(config-if-range)#exit

Paso 5: Configure el S2.

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

Tabla 10: Tareas de configuración VLAN S2

Tarea	Especificación	Comando Ejecutado
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	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
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport mode trunk

		S2(config-if)#switchport trunk native vlan 6 S2(config-if-range)#exit
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(config)# interface range fa0/1-2 S2(config-if-range)#interface port-channel 2 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if-range)#channel-group 2 mode passive S2(config-if-range)#no shutdown S2(config-if-range)#exit
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18	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	permite 3 MAC addresses	S2(config)#interface fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#exit
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	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 Interfaces no utilizadas S2(config-if-range)#shutdown S2(config-if-range)#exit

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11Tareas de configuración DHCP R1

Tarea	Especificación	Comando Ejecutado
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
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	R1#configure terminal R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
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	R1#configure terminal R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.21.5.64 255.255.255.224 R1(dhcp-config)#default-router 10.21.5.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Paso 2: Configurar los servidores

Tabla 12: Congiguraciones de red PCA

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	*ccna-a.net*
Dirección física	*0001.978B.8576*
Dirección IP	*10.21.5.2*
Máscara de subred	*255.255.255.192*

Tabla 13: Configuraciones de red PCB

Descripción	*ccna-b.net*
Dirección física	*00E0.F993.53EC*
Dirección IP	*10.21.5.66*
Máscara de subred	*255.255.255.224*
PC-A Network Configuration	
Gateway predeterminado	*10.21.5.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 14 Resultados de ping

Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	*Packets: Sent = 4, Received = 4*
PC-A	*R1, G0/0/1.2*	IPv6	2001:db5:acad:a::1	*Packets: Sent = 4, Received = 4*
PC-A	R1, G0/0/1.3	Dirección	10.21.5.65	*Packets: Sent = 4, Received = 4*
PC-A	*R1, G0/0/1.3*	IPv6	2001:db5:acad:b::1	*Packets: Sent = 4, Received = 4*
PC-A	R1, G0/0/1.4	Dirección	10.21.5.97	*Packets: Sent = 4, Received = 4*
PC-A	*R1, G0/0/1.4*	IPv6	2001:db5:acad:c::1	*Packets: Sent = 4, Received = 4*
PC-A	S1, VLAN 4	Dirección	10.21.5.98	*Packets: Sent = 4, Received = 4*
PC-A	*S1, VLAN 4*	IPv6	2001:db5:acad:c::98	*No responde*
PC-A	S2, VLAN 4	Dirección	10.21.5.99.	*Packets: Sent = 4, Received = 4*
PC-A	*S2, VLAN 4*	IPv6	2001:db5:acad:c::99	*No responde*
PC-A	PC-B	Dirección	10.21.5.66 (DHCP)	*Packets: Sent = 4,*

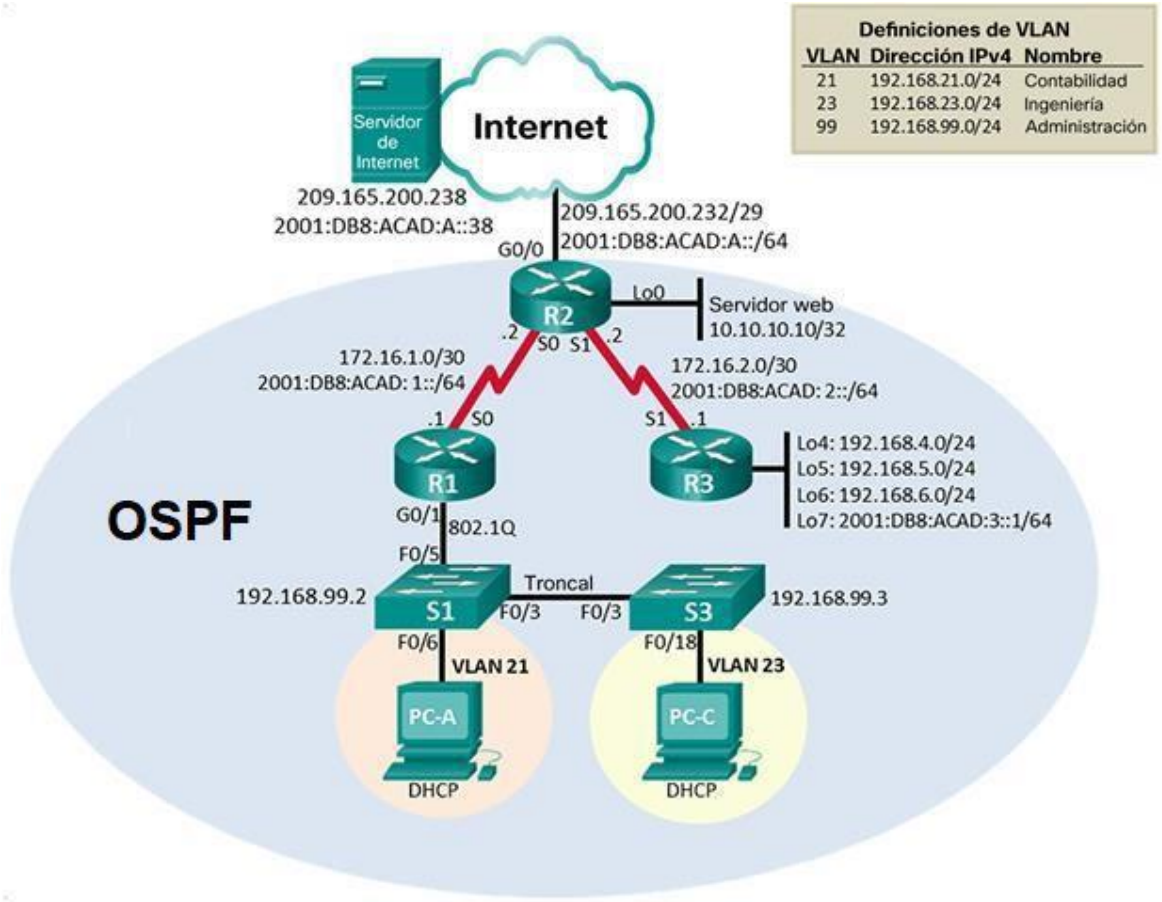
				Received = 4
PC-A	*PC-B*	IPv6	2001:db5:acad:b: :50	*Packets: Sent = 4,* *Received = 4*
PC-A	R1 Bucle 0	Dirección	209.165.201.1	Packets: Sent = 4, Received = 4

Desde	**A**	**de Internet**	**Dirección IP**	**Resultados de ping**
PC-A	*R1 Bucle 0*	IPv6	2001:db5:acad:209: :1	*No responde*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Packets: Sent = 4, Received = 4
PC-B	*R1 Bucle 0*	IPv6	2001:db5:acad:209: :1	*No responde*
PC-B	R1, G0/0/1.2	Dirección	10.21.5.1	*Packets: Sent = 4, Received = 4*
PC-B	*R1, G0/0/1.2*	IPv6	2001:db5:acad:a: :1	*Packets: Sent = 4, Received = 4*
PC-B	R1, G0/0/1.3	Dirección	10.21.5.65	*Packets: Sent = 4, Received = 4*
PC-B	*R1, G0/0/1.3*	IPv6	2001:db5:acad:b: :1	*Packets: Sent = 4, Received = 4*
PC-B	R1, G0/0/1.4	Dirección	10.21.5.97	*Packets: Sent = 4, Received = 4*
PC-B	*R1, G0/0/1.4*	IPv6	2001:db5:acad:c: :1	*Packets: Sent = 4, Received = 4*
PC-B	S1, VLAN 4	Dirección	10.21.5.98	*Packets: Sent = 4, Received = 4*
PC-B	*S1, VLAN 4*	IPv6	2001:db5:acad:c: :98	*No responde*
PC-B	S2, VLAN 4	Dirección	10.21.5.99.	*Packets: Sent = 4, Received = 4*
PC-B	*S2, VLAN 4*	IPv6	2001:db5:acad:c: :99	*No responde*

ESCENARIO 2

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

Figura 7 Topología 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 15 Inicialización de dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable 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 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- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free)

Paso 1: Configurar la computadora de Internet

Parte 2: Configurar los parámetros básicos de los dispositivos

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

Tabla 16 Configuración 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::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configuración 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)#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 unicast-routing

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configuración 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
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)#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)#exit
Interfaz S0/0/1	R2(config)#interface serial 0/0/1 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)#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)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown 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

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 19 Configuración 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)#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)#exit
Interfaz loopback 4	R3(config)#interface lo4

	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)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit.
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing
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 20 Configuración 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 21 Configuración 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 22 Verificación conectividad

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 = 8/16/30 ms
R2	R3, S0/0/1	172.16.2.1	Type escape sequence to abort. 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 = 1/11/16 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Ping statistics for 209.165.200.233:

			Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Figura 8 Ping R1 a R2

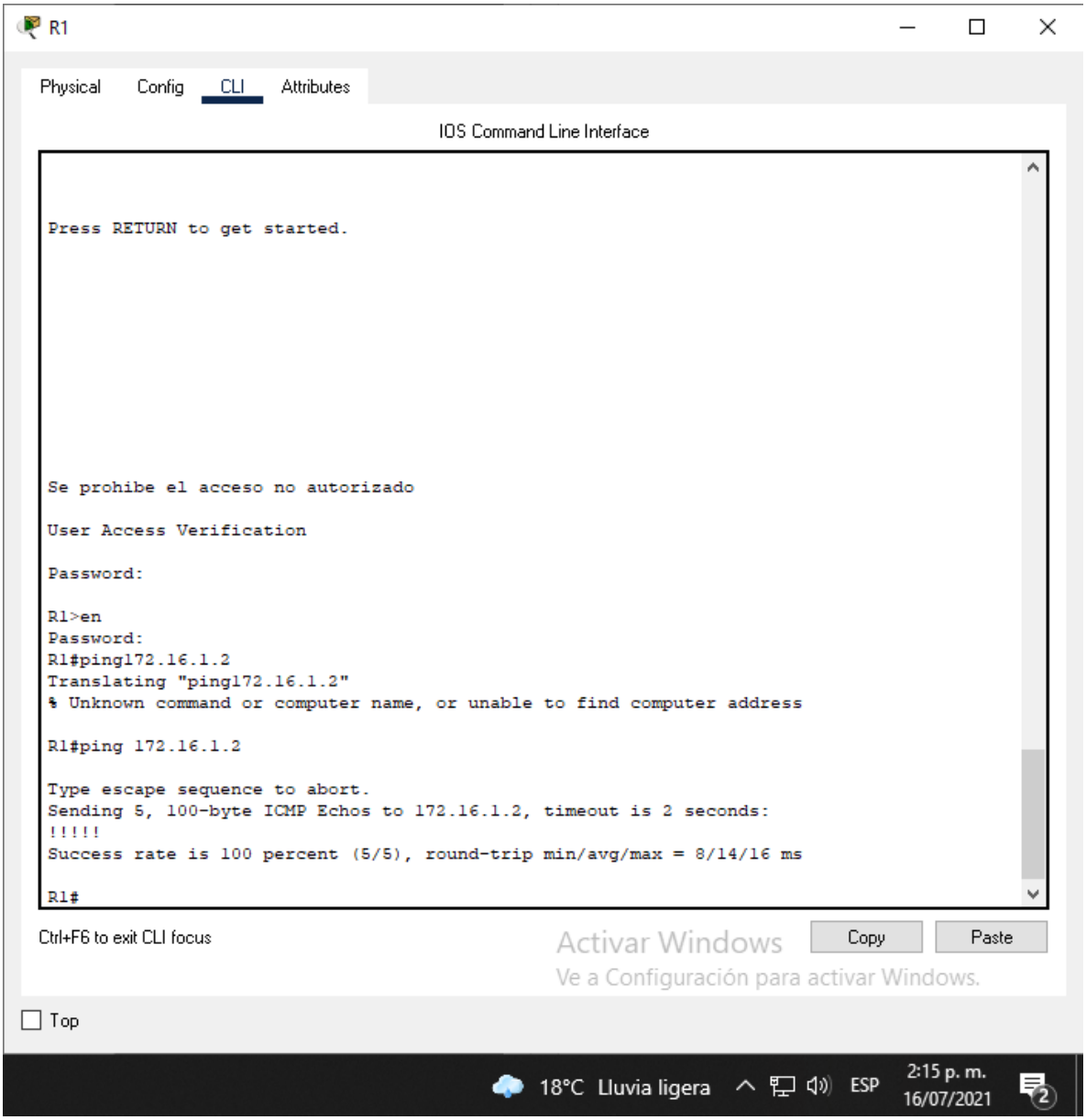


Figura 9 Ping R2 a R3

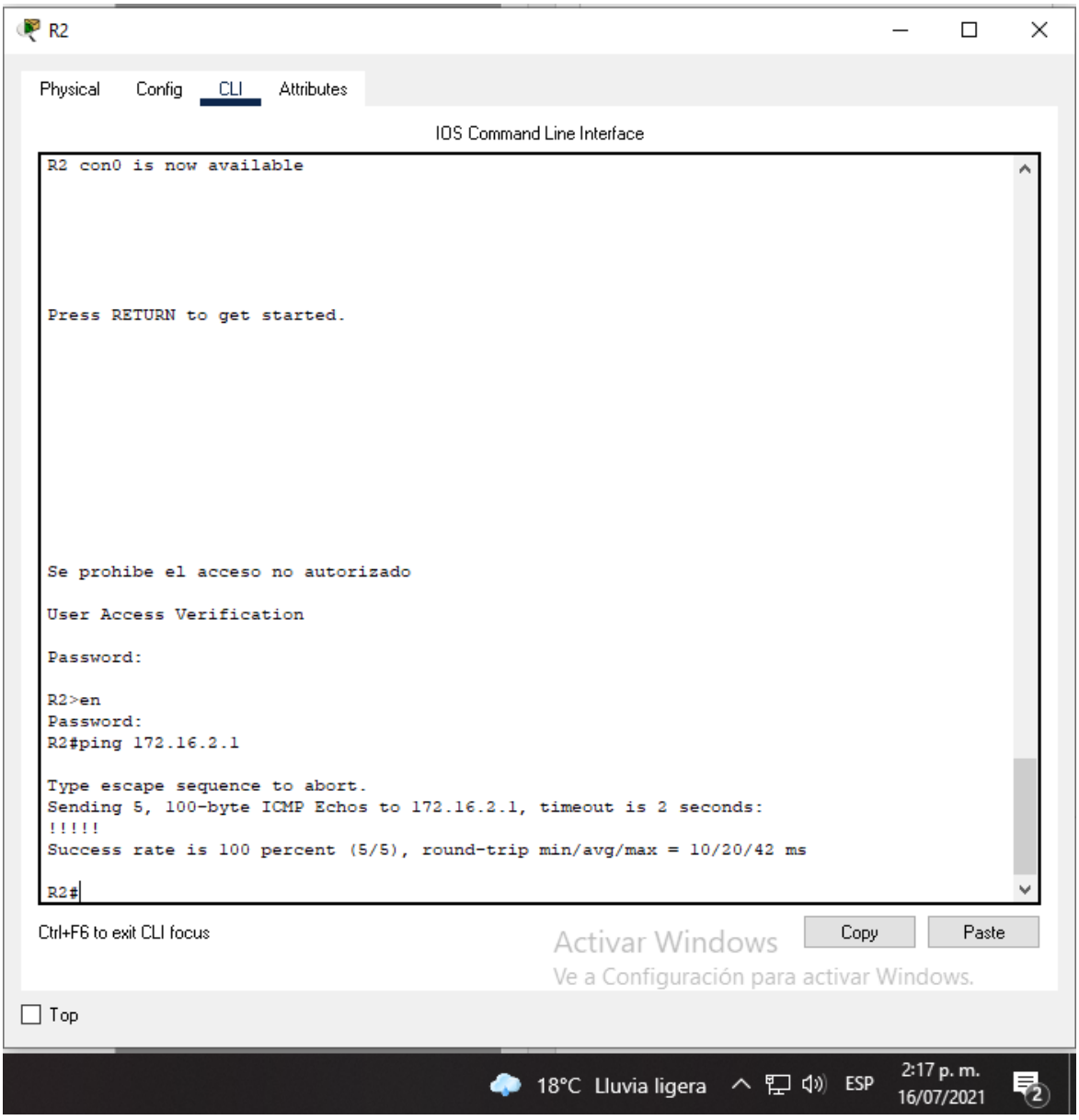
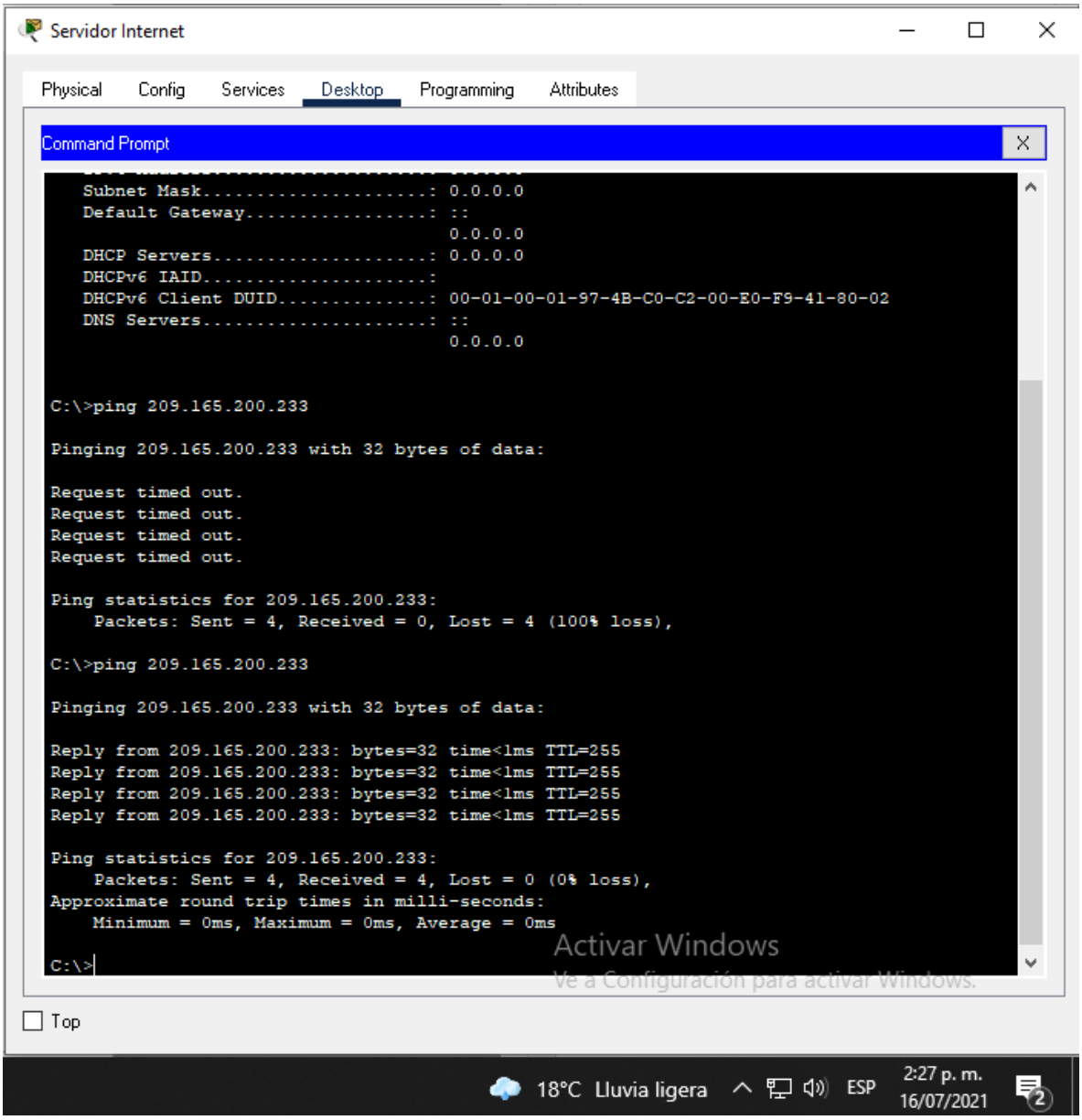


Figura 10 Ping servidor de internet a gateway predeterminado



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 23 Configuración VLAN en 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)#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 24 Configuración VLAN en 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)#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)#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 25 Configuración VLAN en 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)#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)#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)#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 26 Verificación conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	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	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
S1	R1, dirección VLAN 21	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 = 0/3/15 ms
S3	R1, dirección VLAN 23	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 = 0/0/0 ms

Figura 11 Ping S1 a VLAN Administración

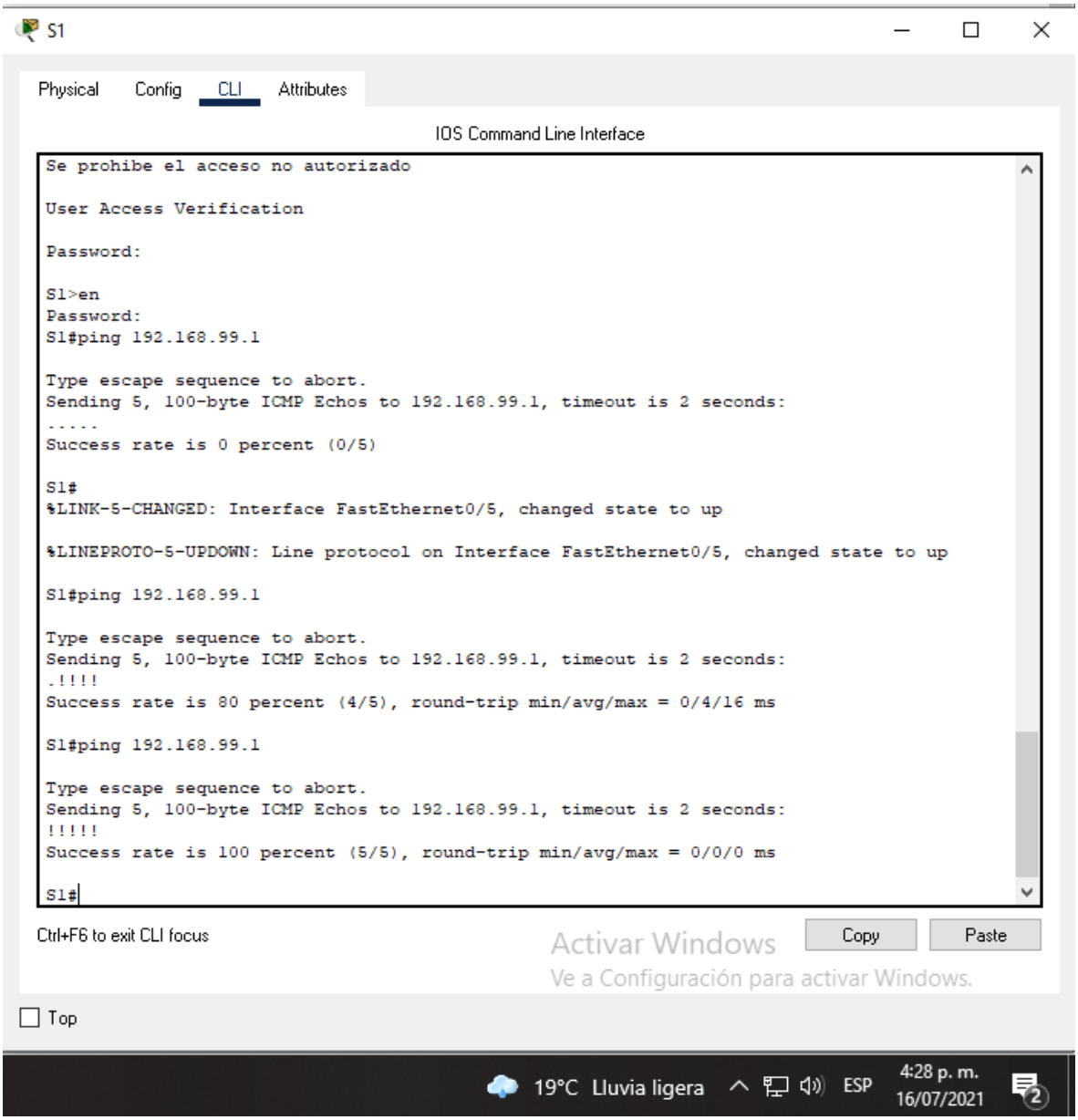


Figura 12 Ping S3 a VLAN Administración

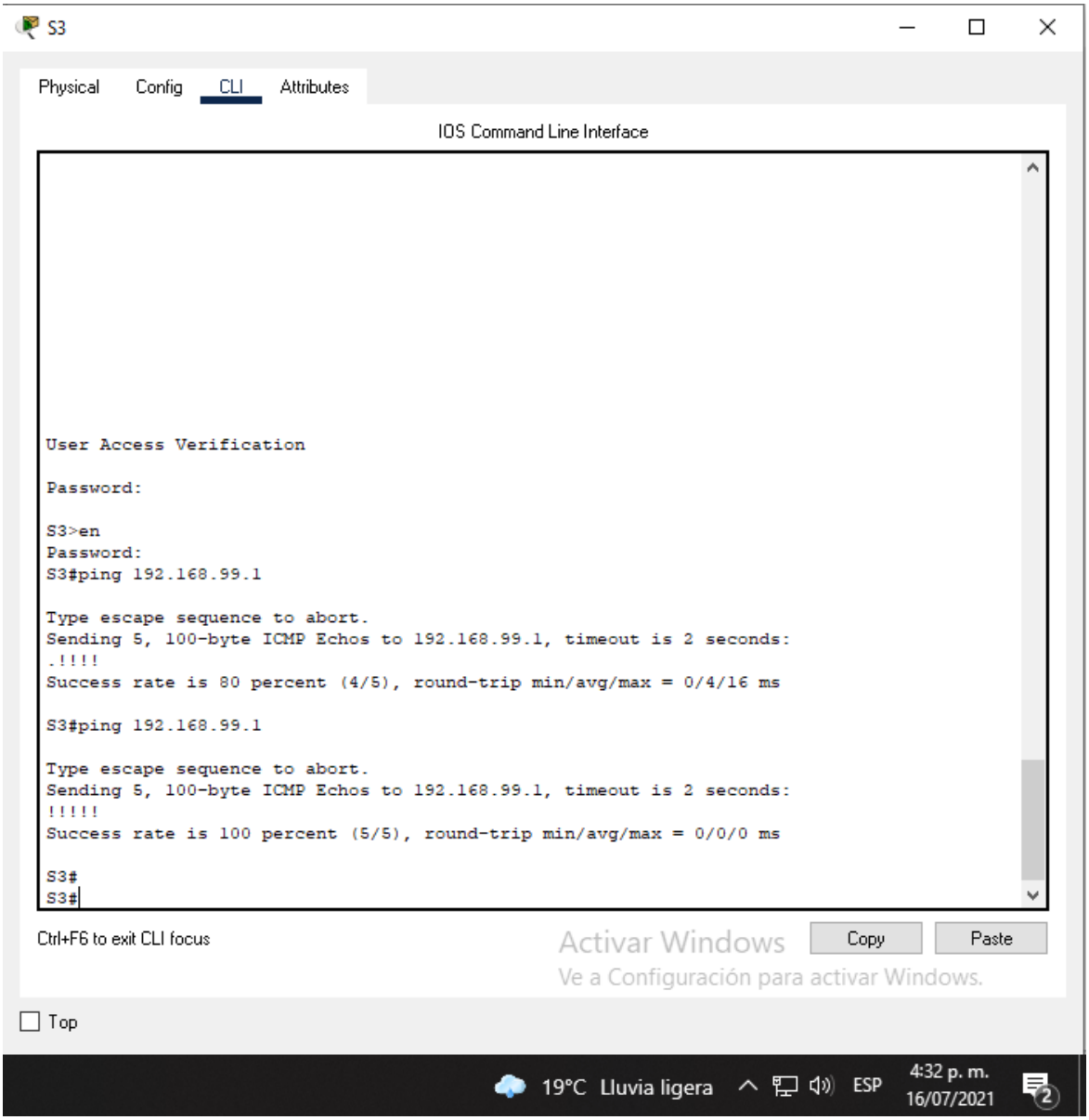


Figura 13 Ping de S1 a VLAN Contabilidad

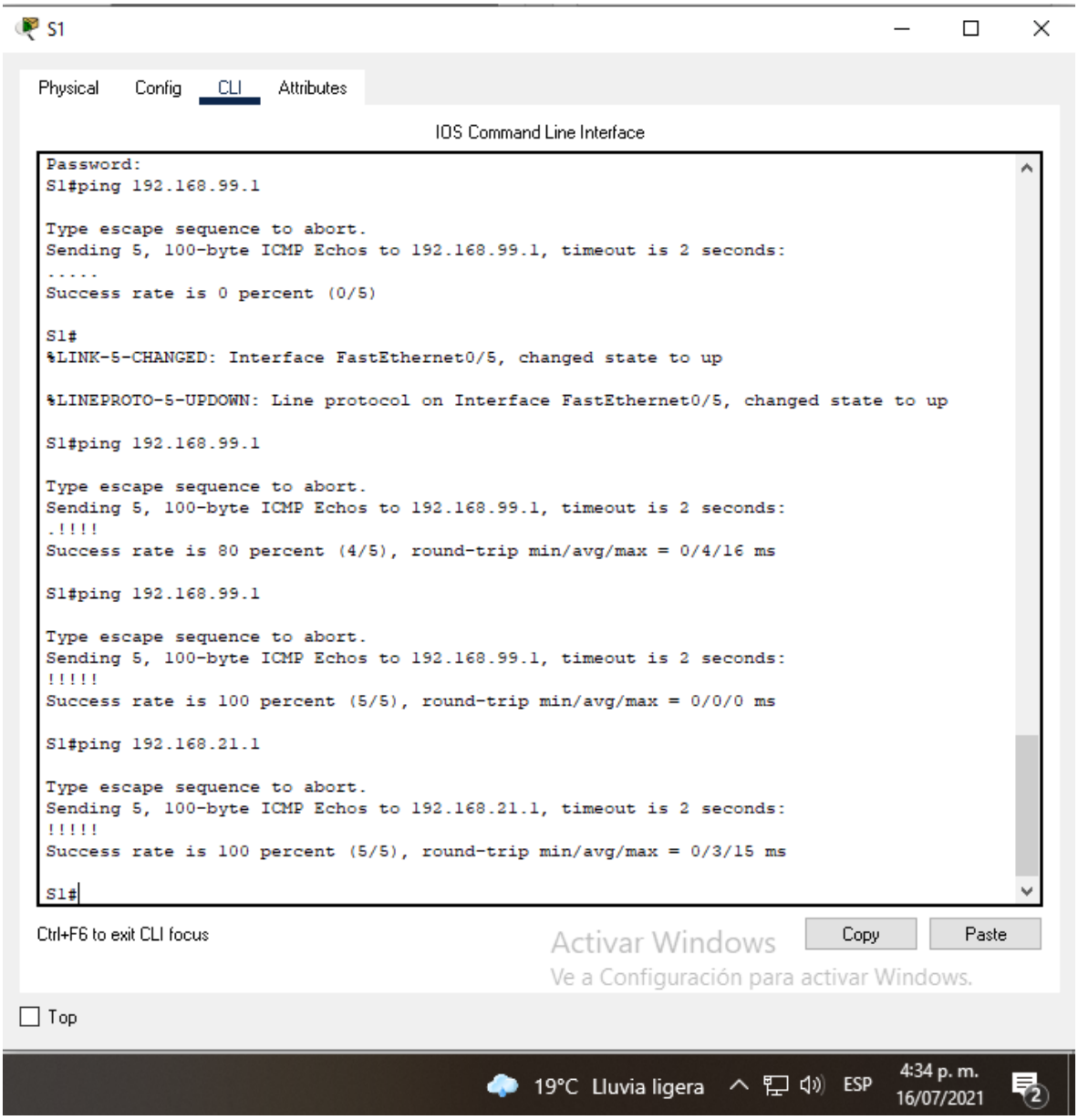
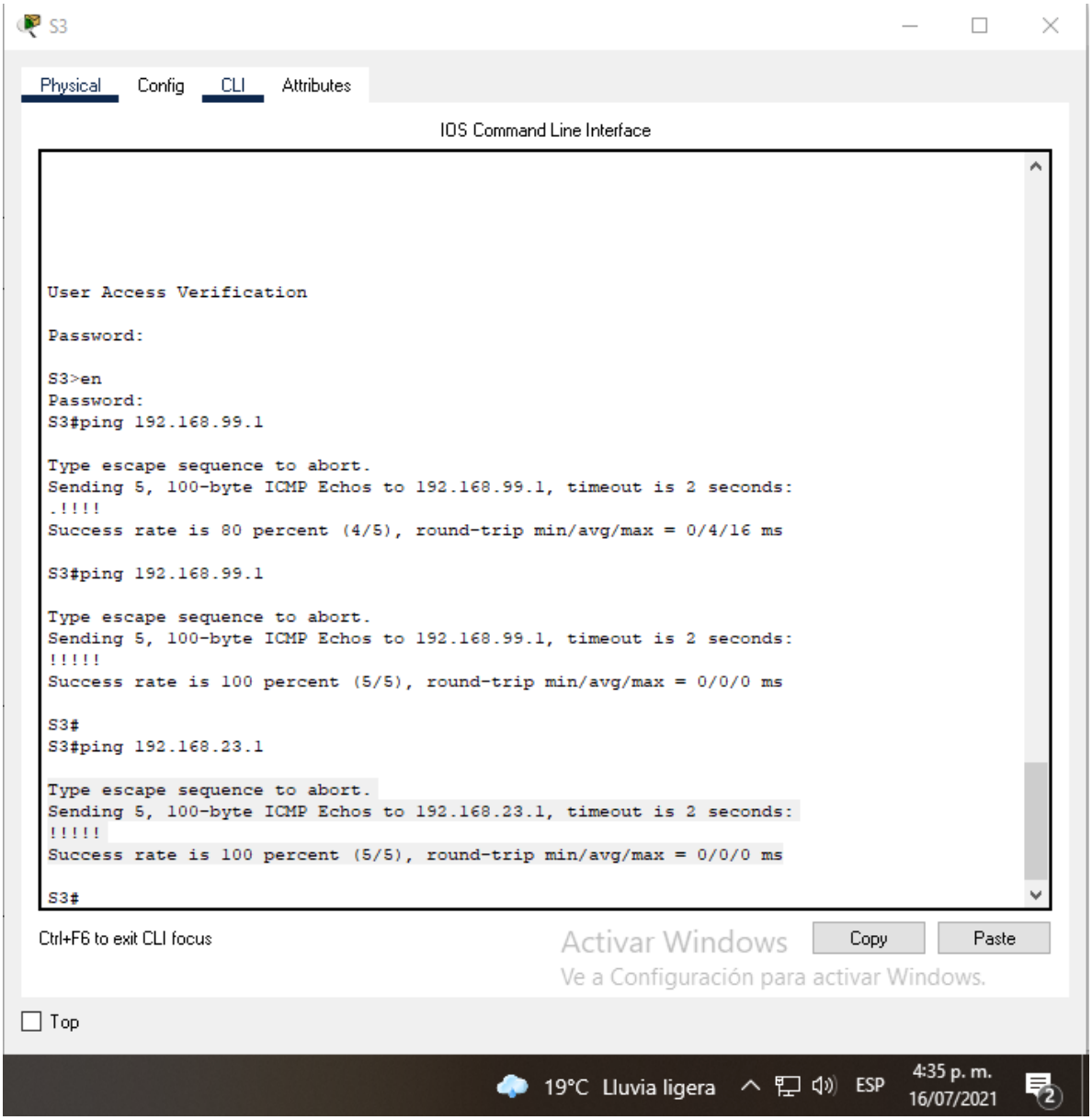


Figura 14 Ping S3 a VLAN Ingeniería



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 27 Configuración OSPF en 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	No se encuentra un comando que funcione en OSPF

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 28 Configuración OSPF en 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.	No se encuentra un comando que funcione en OSPF

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 29 Configuración OSPFv3 en 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.	No se encuentra un comando que funcione en OSPF

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 30 Verificación de información 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?	Con el comando show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Con el comando show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Con el comando show ip ospf database

Figura 15 Información OSPF en R1

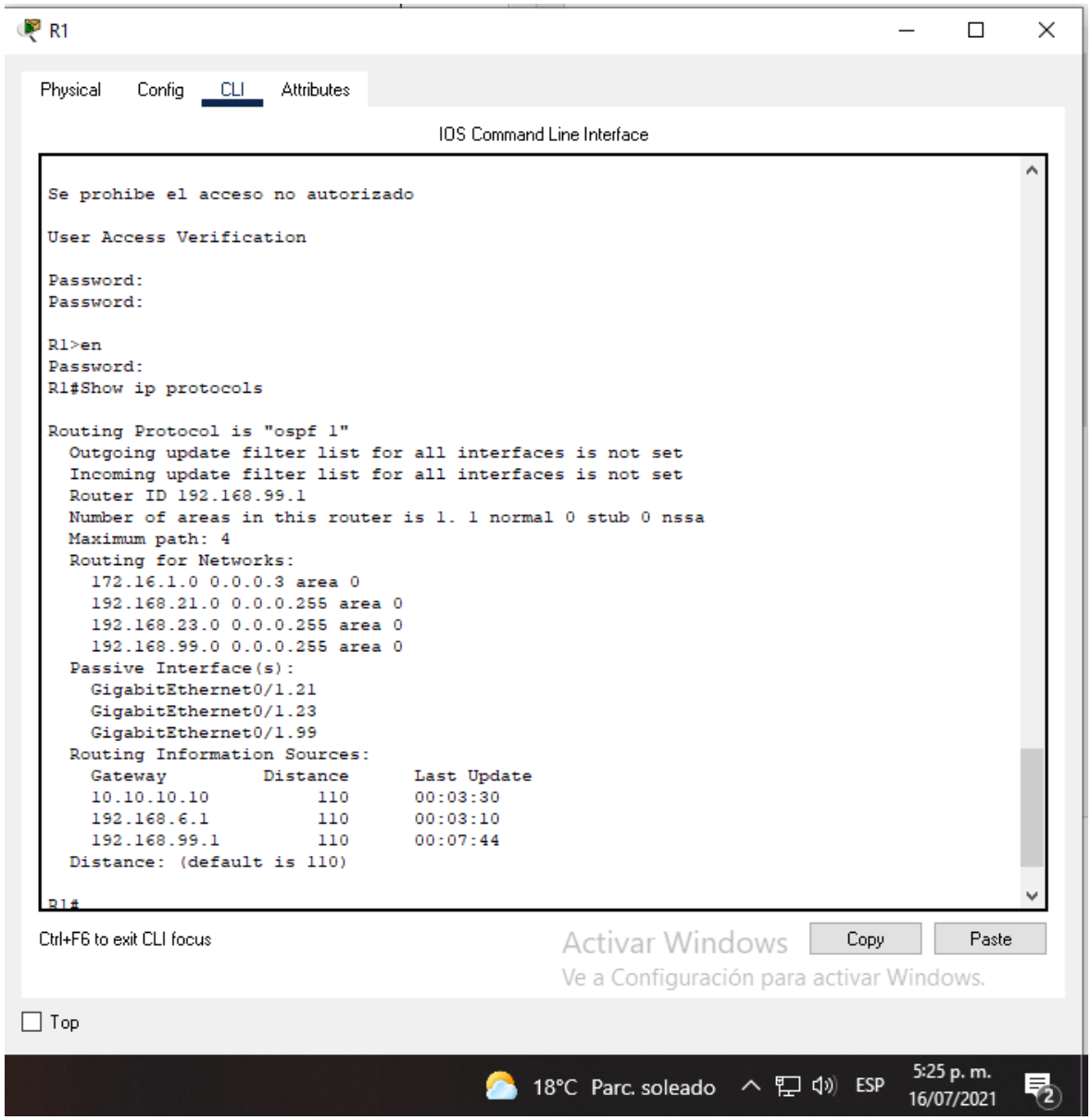


Figura 16 Rutas OSPF en R1

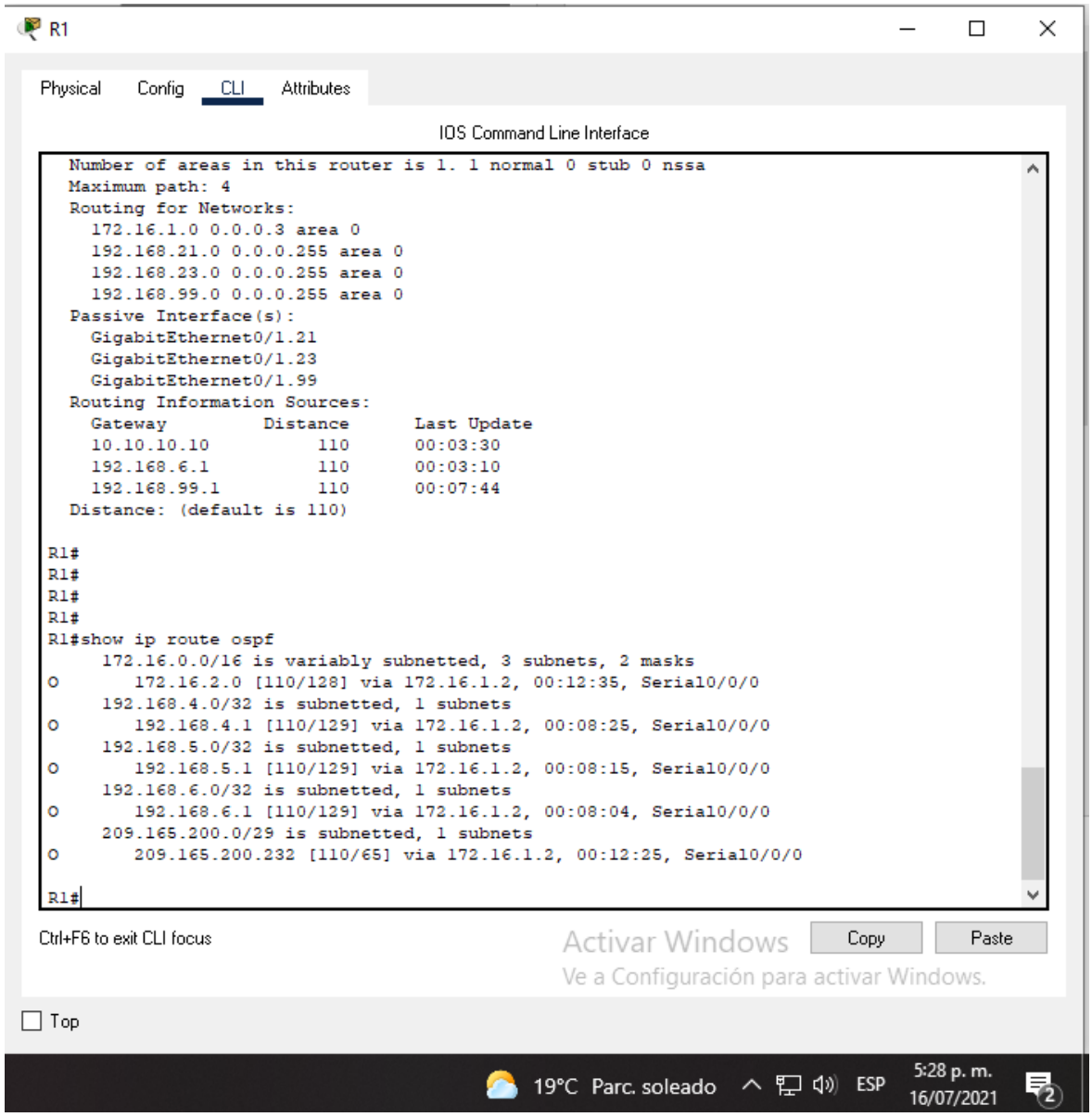
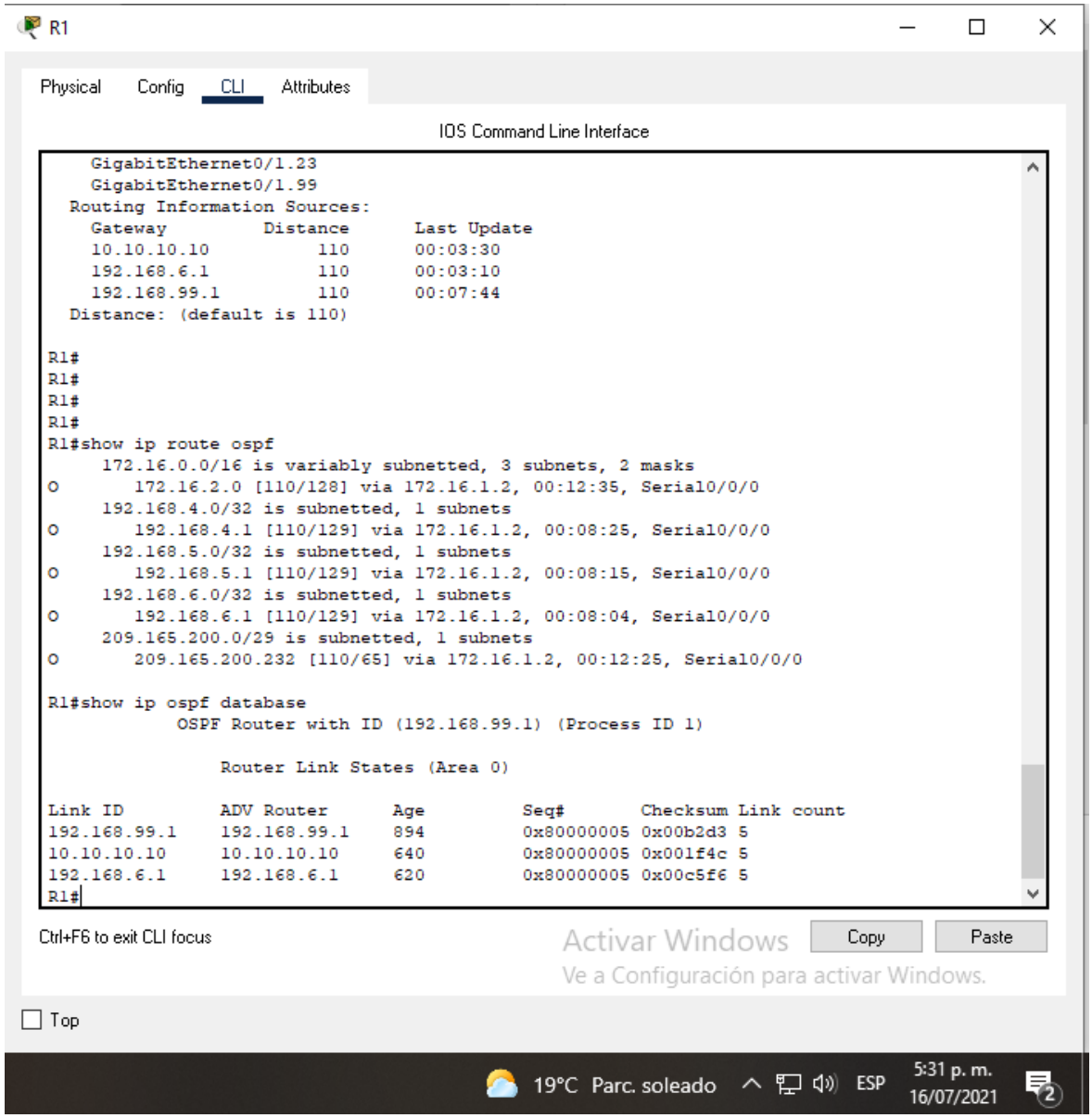


Figura 17 Sección OSPF de la configuración en ejecución del R1



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 31 Configuración R1 como servidor DHCP para las VLAN 21 y 23

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 32 Configuración NAT 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 por packet tracer

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado por packet tracer
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 33 Verificación de protocolo DHCP y NAT

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 (209.165.200.238) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	

Figura 18 Verificación DHCP para PC-A

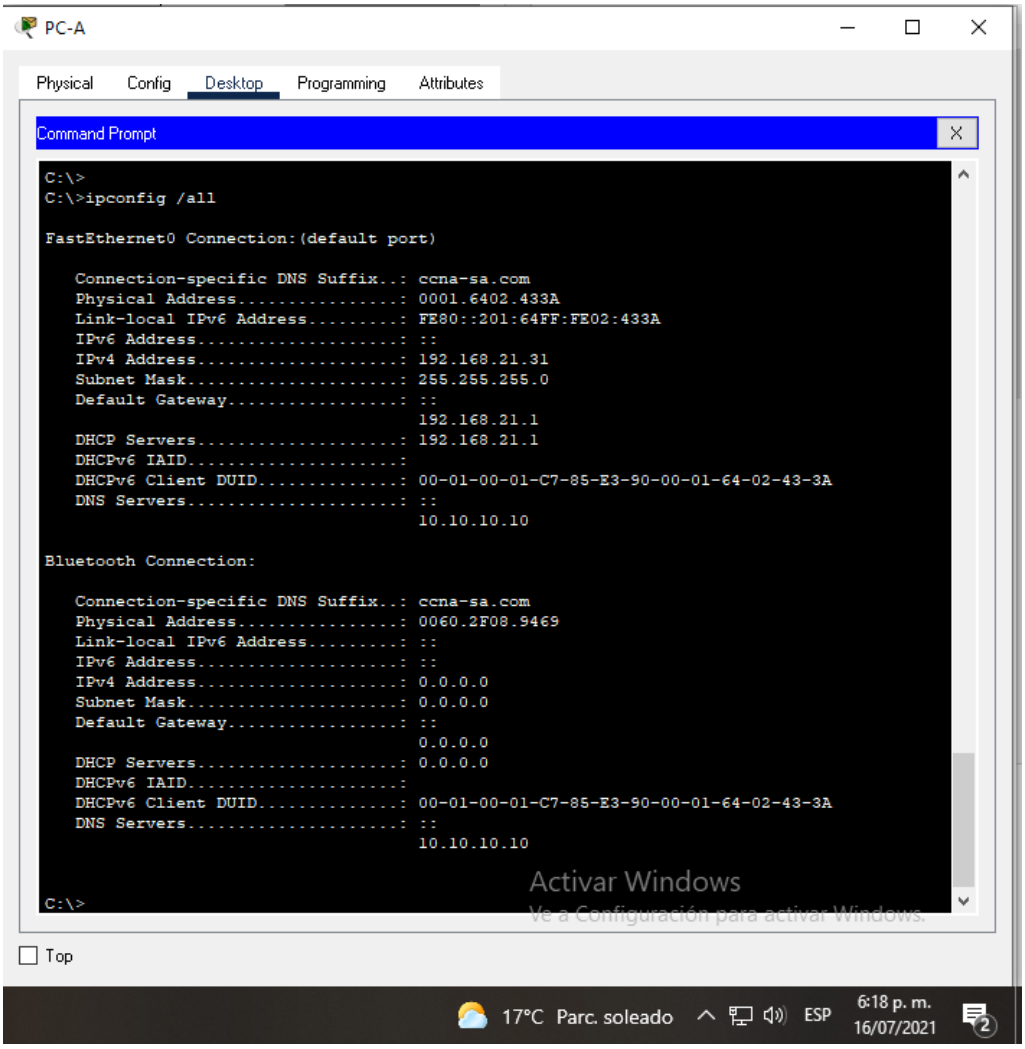


Figura 19 Verificación DCHP para PC-C

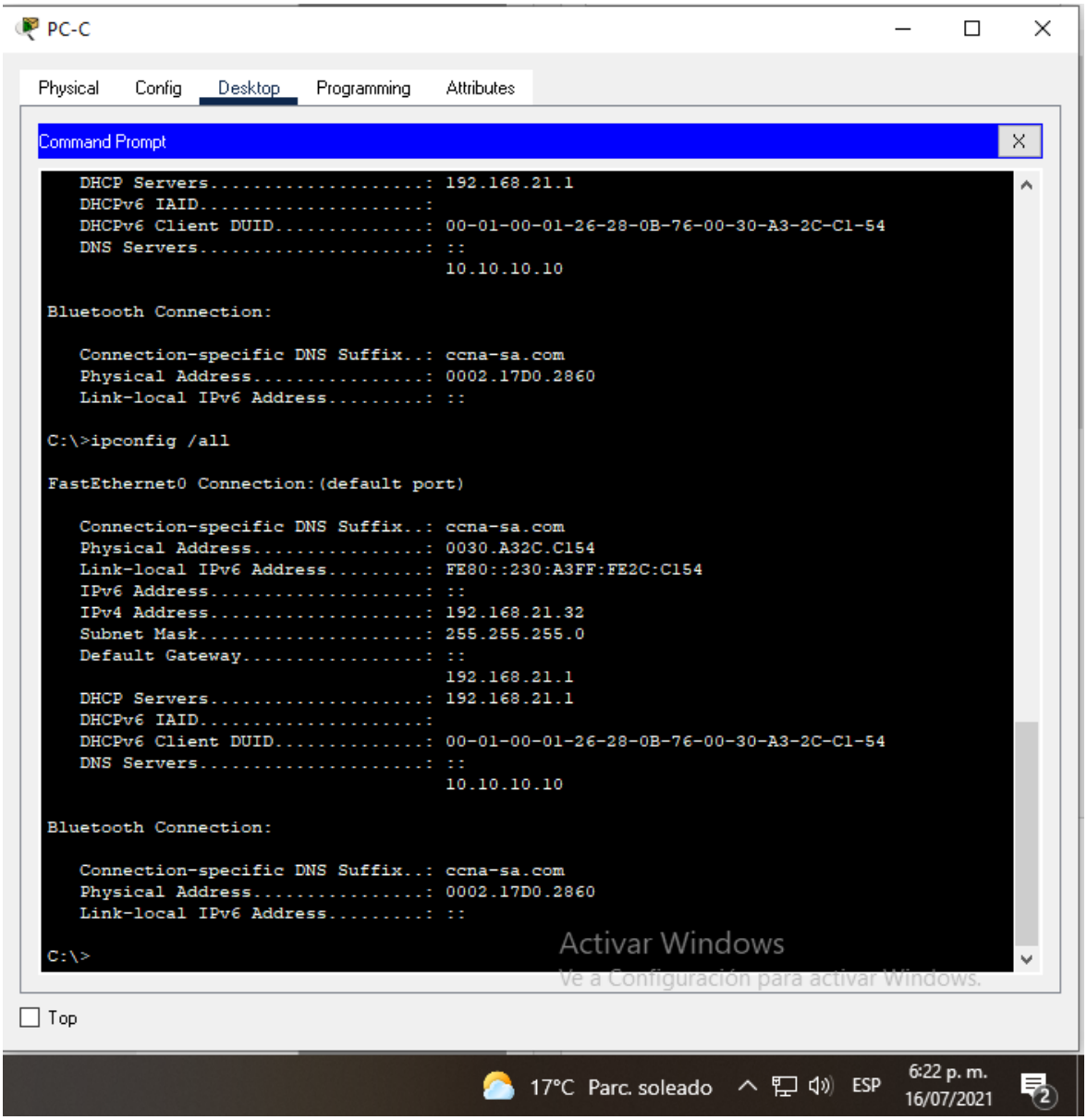


Figura 20 Ping PC-A a PC-C

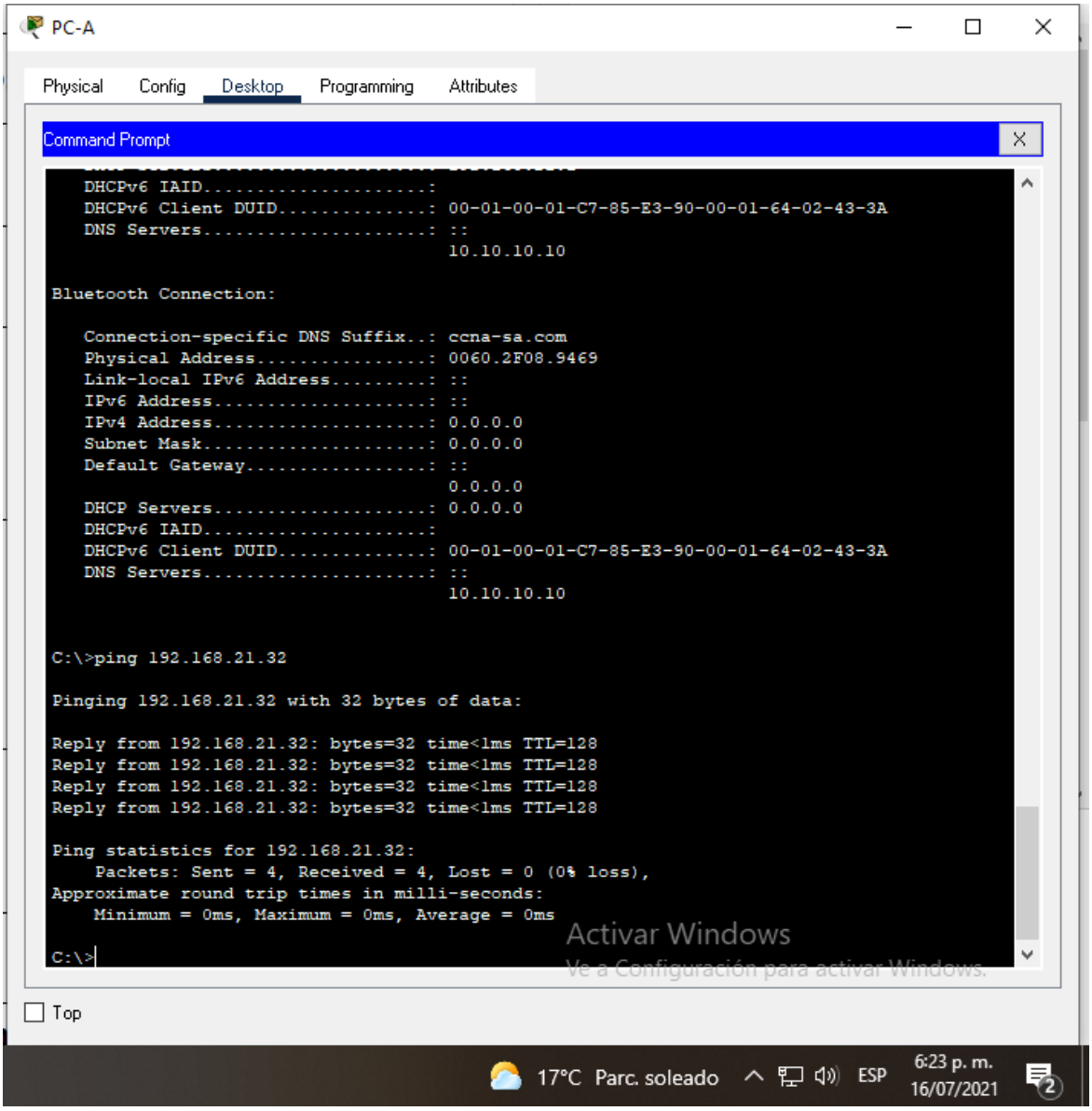
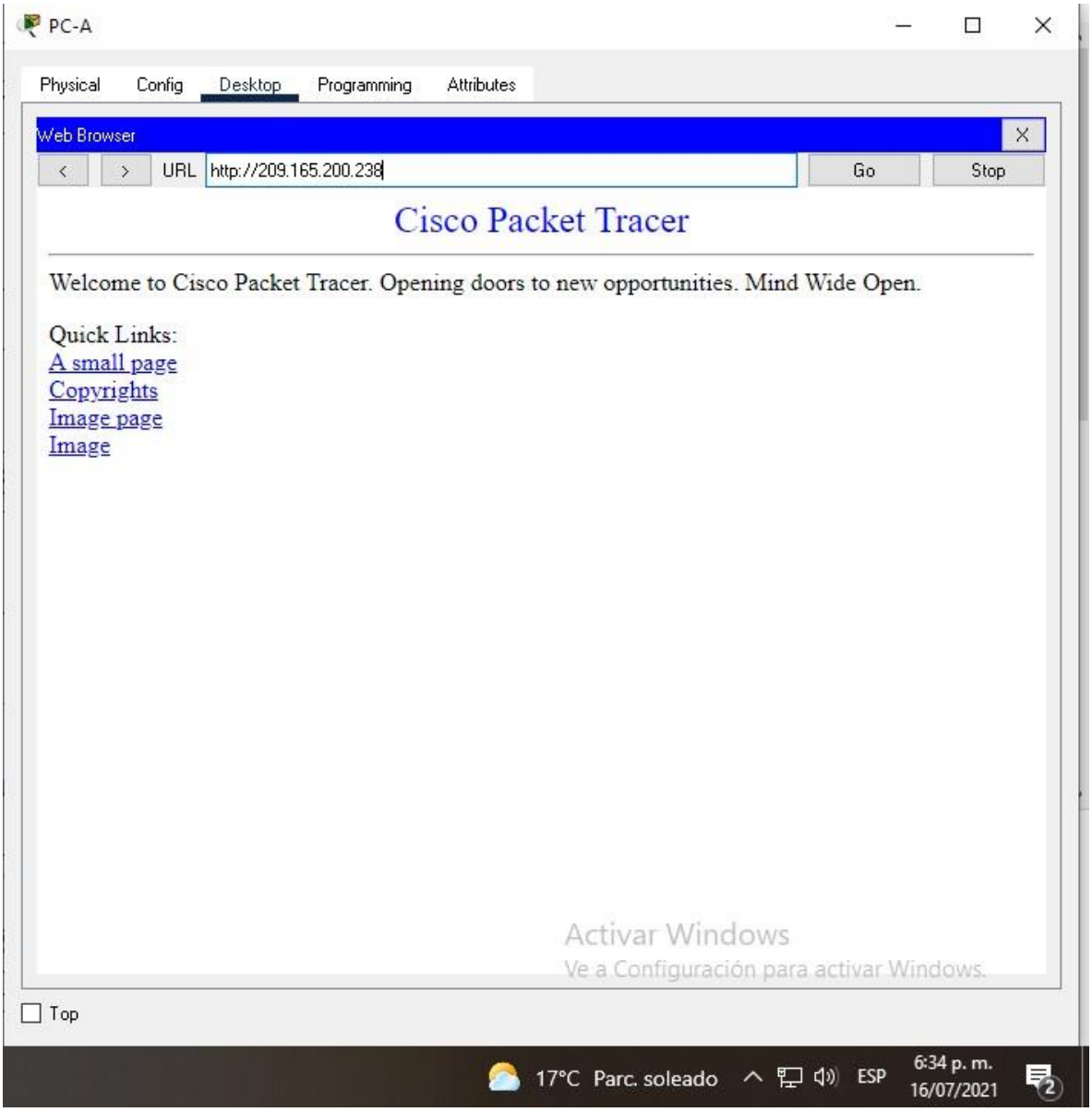


Figura 21 Acceso PC-A a servidor web



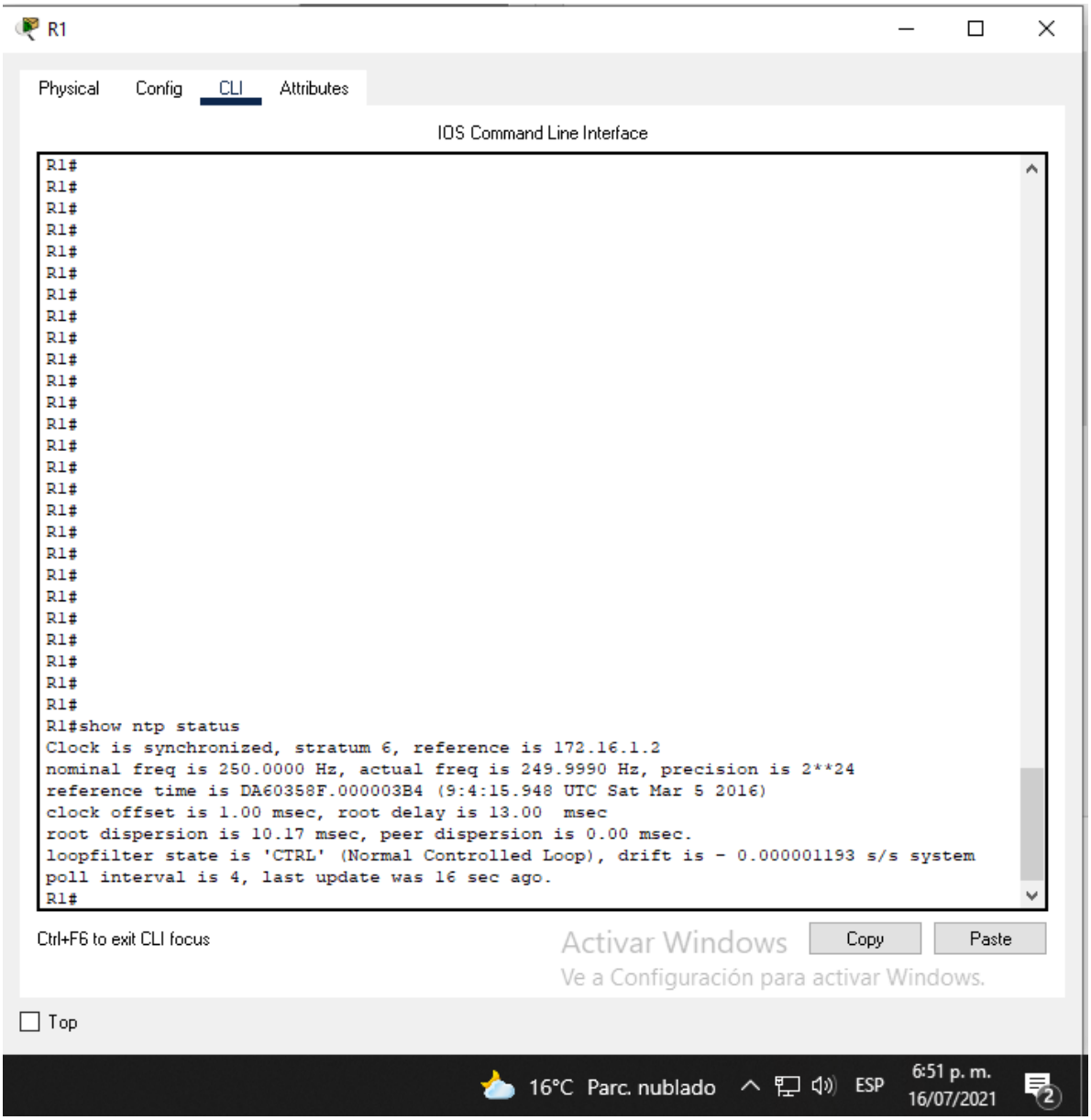
Parte 6: Configurar NTP

Tabla 34 Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 Mar 2016
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 22 Verificación de NTP en R1



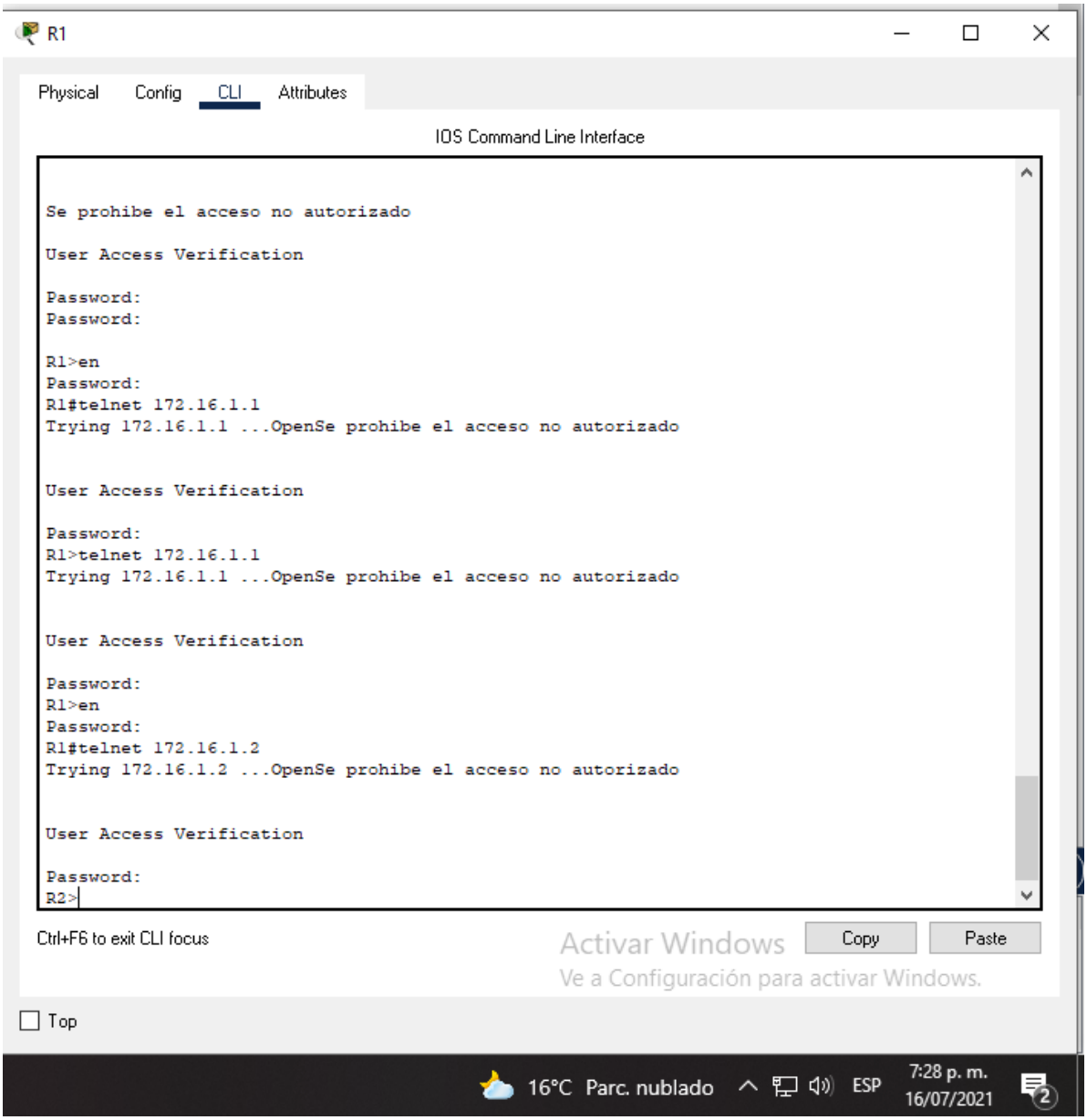
Parte 7: Configurar y verificar las listas de control de acceso (ACL)

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

Tabla 35 Restringir acceso VTY a 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)#access-class ADMIN-MGT in R2(config-line)#exit
Verificar que la ACL funcione como se espera	

Figura 23 Verificación acceso a R2 desde R1



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

Tabla 36 Comandos CLI para información

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
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

CONCLUSIONES

- Según lo observado en el escenario 1, es de vital importancia el entendimiento y comprensión del direccionamiento IP tanto v4 como v6 ya que de este parte las practicas en el diseño y configuración de una red estable y segura

- La herramienta packet tracer complementa la adquisición de conocimientos y ayuda a resolver dudas en la configuración de los diferentes dispositivos.

- Se complementó el uso de comandos CISCO así como su sintaxis y uso adecuado dentro de los dispositivos.

- Se toma una postura más analítica en cuanto a los problemas y errores de red que se presentan.

BIBLIOGRAFIA

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

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

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

- 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). 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