DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

“Solución de dos estudios de caso bajo el uso de tecnología CISCO”

GABRIEL ANTONIO RINCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

COLOMBIA

2021

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

“Solución de dos estudios de caso bajo el uso de tecnología CISCO”

GABRIEL ANTONIO RINCÓN

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

Presentado a:

MSc. Héctor Manuel Herrera Herrera.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

COLOMBIA

2021

Nota de Aceptación

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá, 16 de julio de 2021 (16, 07, 2021)

Dedico este trabajo primordialmente a mi Dios todo poderoso, ya que es gracias a el que se logró alcanzar este sueño.

A mis queridos padres, por todo su sacrificio y esfuerzo apoyándome todos estos años para poder salir adelante con mi carrera.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ACL: Listas de control de acceso, son listas que le indican al router, qué tipo de paquetes aceptar o rechazar en base a las condiciones establecidas en ellas y que permiten la administración del tráfico y aseguran el acceso, bajo esas condiciones, hacia y desde una red.

DHCP: Reduce en gran medida los errores que se producen cuando las direcciones IP se asignan de forma manual, y puede estirar las direcciones IP al limitar el tiempo que un dispositivo puede mantener una dirección IP individual.

GATEWAY: Una puerta de enlace es un nodo (router) en una red de computadoras, un punto clave de detención de datos en su camino hacia o desde otras redes. La dirección de la puerta de enlace (o default gateway) es una interfaz de router conectada a la red local que envía paquetes fuera de la red local.

IPv4: Protocolo de Internet versión 4 (IPv4) es la forma de direccionamiento IP utilizada habitualmente para identificar hosts en una red y utiliza un formato de 32 bits.

IPv6: Protocolo de Internet versión 6 (IPv6) es el estándar de dirección IP de última generación diseñado para sustituir el formato IPv4. IPv6 resuelve el problema de escasez de direcciones mediante el uso de direcciones de 128 bits en lugar de direcciones de 32 bits que se utilizaban en IPv4.

LAN: Una red local es la interconexión de varios computadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

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

NAT ESTÁTICA: Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet.

NAT DINÁMICA: El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

NTP: Network Time Protocol el cual nos permite sincronizar los dispositivos que funcionan en una red.

OSPF: Open Shortest Path First (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP).

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

SWITCH: Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection).

VLAN: 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.

RESUMEN

El desarrollo del presente trabajo consiste en la administración y configuración de dos redes utilizando el software cisco Packet Tracer. Inicialmente se realiza la topología de las redes; seguidamente, se configura la primera red para que admita la conectividad IPv4 e IPv6 para los hots soportados en los dispositivos que conforman la red routers, switchs y equipos, el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. En la segunda red se configura también para que admita conectividad IPv4 e IPv6, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), las listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. A medida que se realizan las configuraciones se verifica la comunicación extrema a extremo entre los dispositivos y se comprueban las configuraciones.

Palabras clave: Cisco, Configuración, Enrutamiento, Protocolos, Red.

ABSTRACT

The development of this work consists of the administration and configuration of two networks using the Cisco Packet Tracer software. Initially, the topology of the networks is carried out; Next, the first network is configured to support IPv4 and IPv6 connectivity for the hots supported in the devices that make up the network, routers, switches, and computers, routing between VLANs, DHCP, Etherchannel, and port-security. The second network is also configured to support IPv4 and IPv6 connectivity, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), Static and Dynamic Network Address Translation (NAT), Control Lists Server / Client Access Protocol (ACL) and Network Time Protocol (NTP). As the configurations are made, end-to-end communication between the devices is verified and the configurations are verified.

Keywords: Cisco, Configuration, Routing, Protocols, Network.

INTRODUCCIÓN

La gestión de redes LAN/WAN es primordial hoy en día para garantizar una óptima comunicación entre las empresas, los trabajadores y los clientes, debido a esto es importante que las empresas implementen sistemas de comunicación efectivos, con el fin de disminuir y controlar los riesgos presentes con el manejo de la información.

El presente informe tendrá como objetivo administrar redes LAN/WAN, basadas en requerimientos habituales en las organizaciones para realizar el transporte de la información y asimismo se administrará con el fin de poner en práctica lo aprendido durante el diplomado. Inicialmente se identificará la red, su topología y requerimientos de configuraciones en los dispositivos que conforman la red. Se realizará una investigación bibliográfica sobre la conectividad IPv4 e IPv6, además del enrutamiento entre VLAN, Etherchannel y port-security. Se utilizarán según corresponda los protocolos DHCP, OSPF, NTP, la traducción de direcciones de red dinámicas y estáticas, las listas de control de acceso y se realizarán las configuraciones básicas de los dispositivos, se verificará la conexión y comunicación de cada red mediante los comandos comunes de CLI.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Configurar redes LAN/WAN por medio de herramientas de simulación y laboratorios de acceso remoto con el fin de realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, mediante el uso de comandos especializados en gestión de redes.
- Realizar la configuración de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.
- Configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.
- Diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.
- Verificar las configuraciones, las conexiones y la comunicación entre los dispositivos que conforman cada una de las redes.

3. DESARROLLO DE LA PRUEBA DE HABILIDADES

3.1 ESCENARIO 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Se 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.

Topología

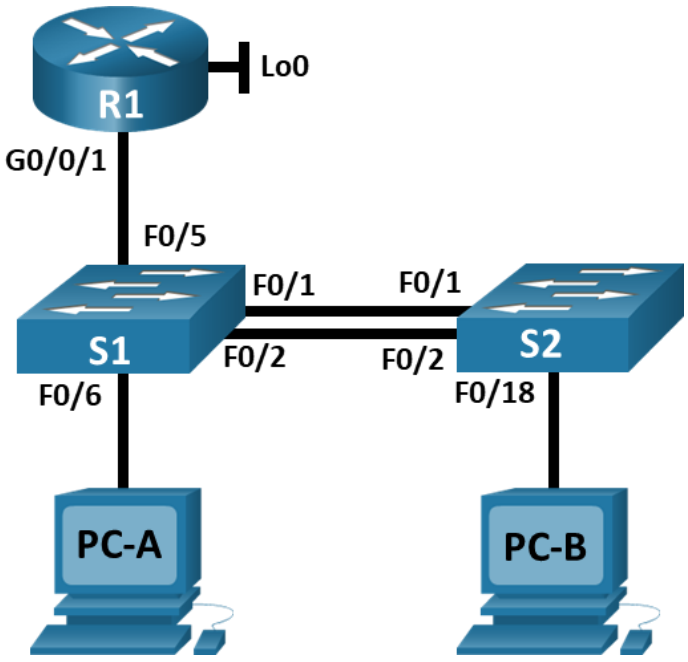

Figura 1 Topología del primer escenario. Fuente: cisco

Para realizar la topología, primero agregamos a la pantalla principal del software un router 1941, dos switch 3560-24PT y dos equipos de cómputo que se conectaran por medio del cable de cobre directo según corresponda, como muestra la topología.

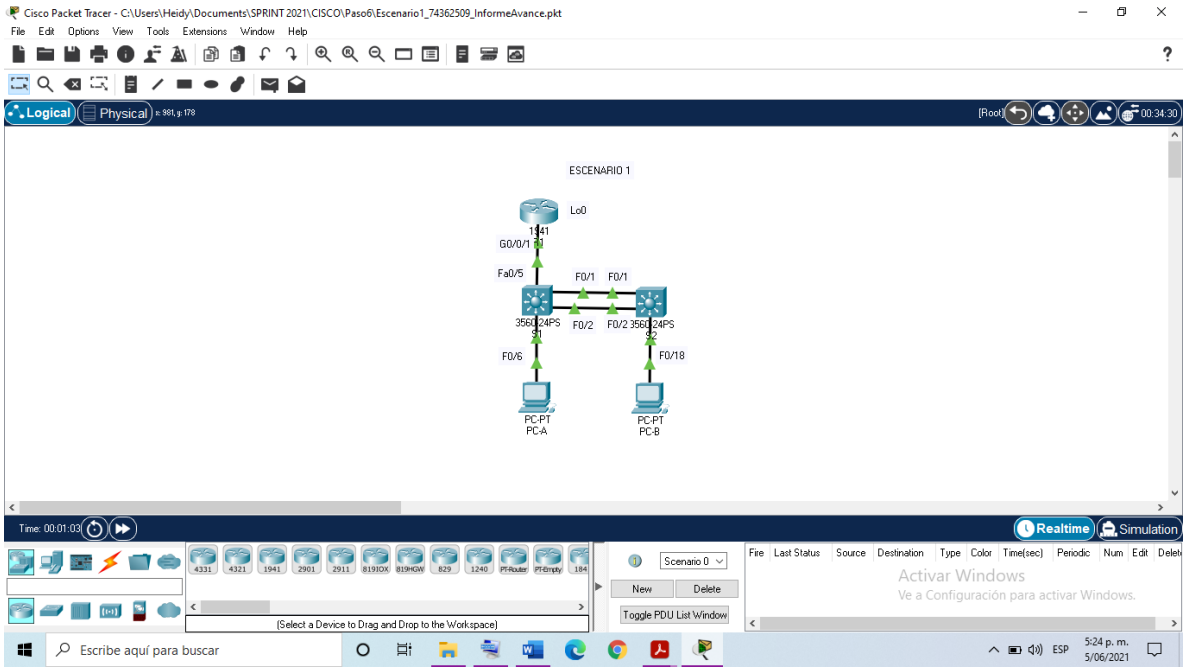

Figura 2 Escenario 1 en el software cisco packet tarcer. Fuente: propia

A continuación, la tabla nos muestra las cinco VLAN que se van a crear en el switch S2, con el correspondiente nombre que se le asignara.

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

Tabla 1. Asignación de las VLAN a crear

En la siguiente tabla, se encuentran las direcciones IPv4 e IPv6 correspondientes a cada dispositivo de la red y la puerta de enlace predeterminada que se configuraran a lo largo del desarrollo del primer escenario.

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

Tabla 2 Asignación de Direcciones IP en los dispositivos

EL procedimiento de configuración de la red, se realiza por medio de cada una de las partes y pasos que se desarrollan a continuación:

PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

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

Borrar las configuraciones de inicio y las VLAN del router y del switch y volver a cargar los dispositivos, por medio de la ejecución de los siguientes comandos tal como se muestra para cada uno de los dispositivos de la red que tenemos en la

figura 1. Para ello se ingresa a cada dispositivo dando doble clic y a través de la ventana (CLI), ingresamos el comando enable, que permite cambiar el modo EXEC del usuario al modo EXEC privilegiado donde si podemos realizar las configuraciones del dispositivo, luego ingresamos el comando erase startup-config para eliminar el contenido de la NVRAM y por último ingresamos el comando reload para reiniciar el dispositivo.

R1

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

Router#

Router#reload

Proceed with reload? [confirm]

S1

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

Switch#

Switch#reload

Proceed with reload? [confirm]

S2

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

Switch#

Switch#reload

Proceed with reload? [confirm]

Después de recargar el switch, se configura la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch, por medio del comando sdm prefer dual-ipv4-and-ipv6 default

Ingresamos a los switch S1 y S2, colocamos el comando enable para ingresar al modo EXEC privilegiado, luego el comando configure terminal para entrar a configurar y colocar el comando sdm prefer dual-ipv4-and-ipv6 default, por último, escribimos el comando reload para activar la nueva configuración.

S1

Switch>enable

Switch#configure terminal

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default

Switch(config)#exit

Switch#reload

System configuration has been modified. Save? [yes/no]: yes

S2

Switch>enable

Switch#configure terminal

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default

Switch(config)#exit

Switch#reload

System configuration has been modified. Save? [yes/no]: yes

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes líneas de comandos y además se crean las subinterfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6 como se asignó en la tabla1, y además se genera una clave de cifrado RSA.

Tarea	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal

	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 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 está prohibido#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface gi0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN to VLAN2 R1(config-subif)#ip add 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit

	R1(config)#interface gi0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description LAN to VLAN3 R1(config-subif)#ip add 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db5:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit
	R1(config)#interface gi0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description LAN to VLAN4 R1(config-subif)#ip add 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db5:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit
	R1(config)#interface gi0/1.6 R1(config-subif)#encapsulation dot1q 6
	R1(config)#interface gi0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1(config)#interface lo0 R1(config-if)#description LAN to Loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db5:acad:209::1/64 R1(config-if)#ipv6 add FE80::1 link-local
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa

Tabla 3 Configuraciones básicas en R1

Paso 2: Configurar S1 y S2.

Las tareas de configuración incluyen las siguientes líneas de comandos y además se crean las subinterfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH, primero comenzamos configurando a S1.

Tarea	**Especificación**
Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)# banner motd #El acceso no autorizado esta prohibido#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 4 S1(config-if)#ip add 10.21.5.98 255.255.255.248 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	S1(config)#ip default-gateway 10.21.5.97 S1(config)#do write

Tabla 4 Configuraciones básicas en S1

Configuración S2.

Tarea	Especificación
Desactivar la búsqueda DNS.	S2(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line con 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip add 10.21.5.99 255.255.255.248 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	S2(config)#ip default-gateway 10.21.5.97 S1(config)#do write

Tabla 5 Configuraciones básicas en S2

PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal S1(config)#interface fa0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk allowed vlan 2,3,4,6 S1(config)#interface fa0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if-range)#switchport trunk allowed vlan 2,3,4,6 S1(config-if)#exit S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if-range)#switchport trunk allowed vlan 2,3,4,6 S1(config-if)#exit

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#channel-protocol lacp S1(config#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#interface fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Puertos sin utilizar S1(config-if-range)#shutdown

Tabla 6 Configuración de la infraestructura de red en S1

Paso 2: Configurar S2

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

Tarea	**Especificación**
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q

	S2(config-if-range)#switchport mode trunk native vlan 6 S2(config-if-range)#switchport trunk allowed vlan 2,3,4,6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface port-channel 2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown S2(config)#interface port-channel 2 S2(config-if-range)#channel-protocol lacp S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit S2(config)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	S2(config)#interface fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Puertos no utilizados S2(config-if-range)#shutdown

Tabla 7 Configuración de la infraestructura de red en S2

PARTE 3: CONFIGURAR SOPORTE DE HOST

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	**Especificación**
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)# ipv6 route ::/0 loopback 0

Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool vlan2 R1(config)#ip dhcp excluded-address 10.21.5.2 10.21.5.52 R1(dhcp-config)# network 10.21.5.0 255.255.255.192 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net1
Configurar DHCP IPv4 para VLAN 3	R1(config)# ip dhcp excluded-address 10.21.5.65 10.21.5.84 R1(config)#ip dhcp pool vlan3 R1(dhcp-config)# network 10.21.5.64 255.255.255.224 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-b.net R1(config)#default-router 10.21.5.65

Tabla 8 Configuración del soporte de host en R1

Paso 4: 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.**

En los equipos PC-A y PC-B se activa el DHCP para IPv4 y configuración automática para IPv6.

PC-A Network Configuration	
Descripción	CCNA-a.net
Dirección física	0000.0c89.3578
Dirección IP	10.21.5.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Tabla 9 Configuración del servidor PC-A

Configuración de red de PC-B	
Descripción	en blanco
Dirección física	00D0.BCDC.3ADB
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Tabla 10 Configuración del servidor PC-B

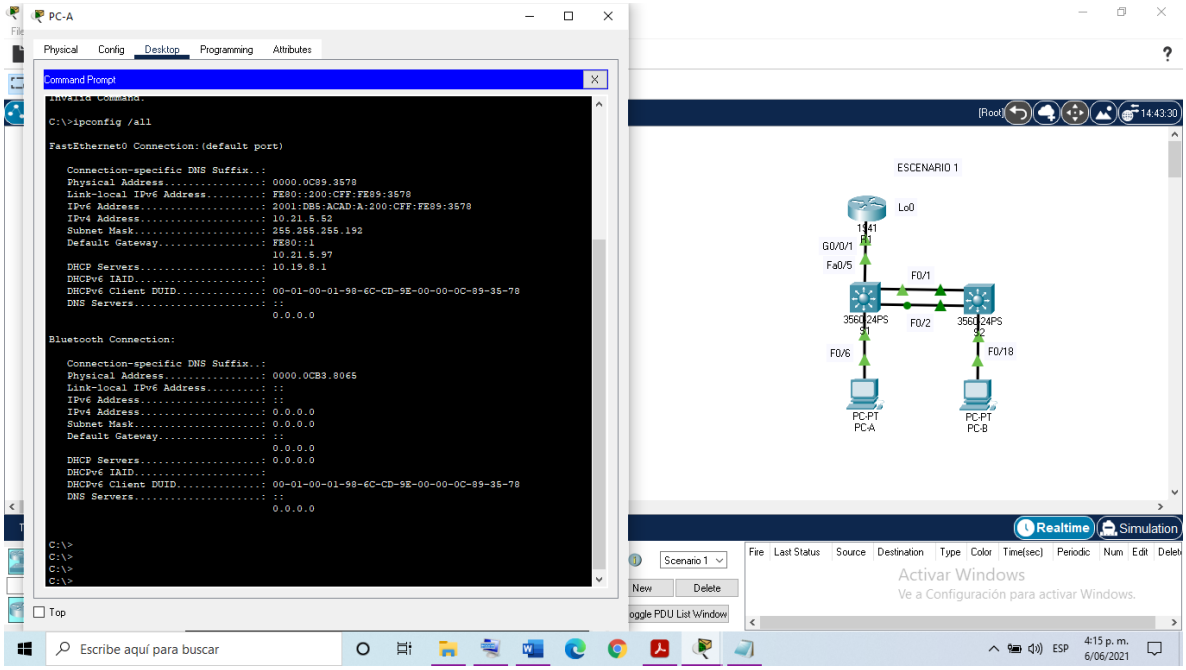

Figura 3 Verificación de la configuración de red de PC-A. Fuente: propia

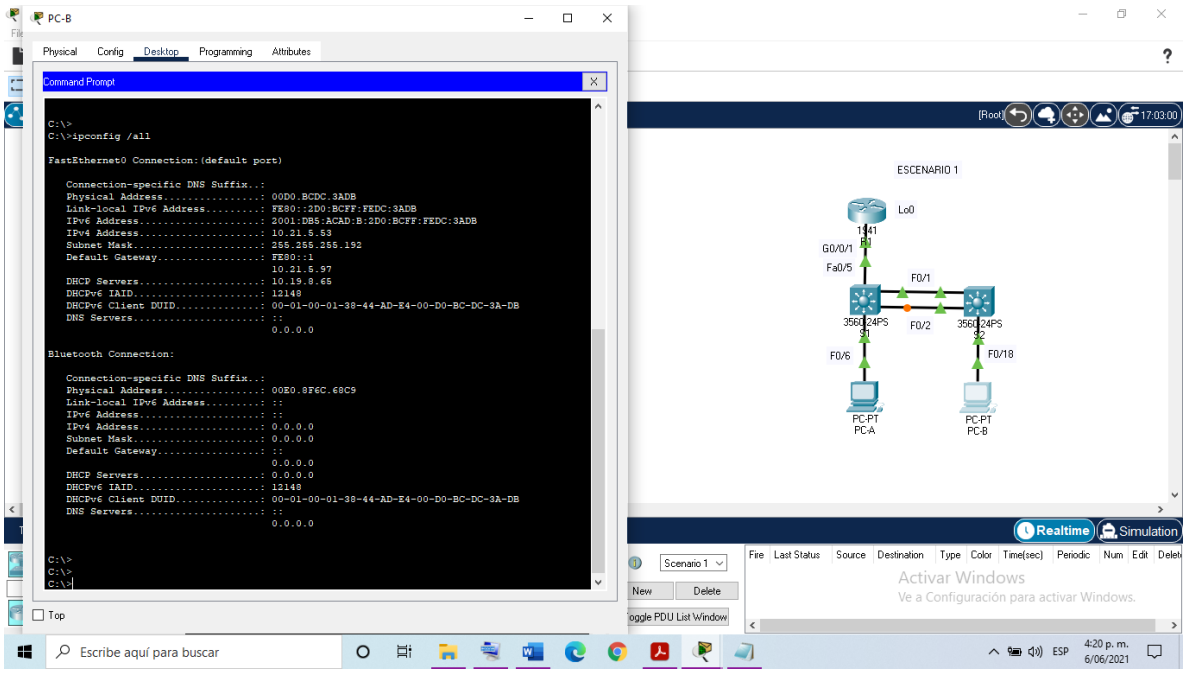

Figura 4 Verificación de la configuración de red de PC-B. Fuente: propia

PARTE 3: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Por medio del comando ping podemos probar la conectividad IPv4 e IPv6 entre todos 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	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	Reply from 10.21.5.1: bytes=32 time=3ms TL=255
	R1, G0/0/1.2	IPv6	2001:db5:acad:a::1	Reply from 2001:db5:acad:a::1: bytes=32 time=1ms TL=255
	R1, G0/0/1.3	Dirección	10.21.5.65	Reply from 10.21.5.65:bytes=32 time=3ms TL=255
	R1, G0/0/1.3	IPv6	2001:db5:acad:b::1	Reply from 2001:DB5:ACAD:B::1: bytes=32 time=1ms TTL=255

	R1, G0/0/1.4	Dirección	10.25.5.97	Reply from 10.25.5.97: bytes=32 time=1ms TTL=255
	R1, G0/0/1.4	IPv6	2001:db5:acad:c::1	Reply from 2001:db5:acad:c::1 bytes=32 time<1ms TTL=255
	S1, VLAN 4	Dirección	10.21.5.98	Reply from 10.21.5.98: bytes=32 time=2ms TTL=254
	S1, VLAN 4	IPv6	2001:db5:acad:c::98	Reply from 2001:db5:acad:c::98 bytes=32 time=2ms TTL=254
	S2, VLAN 4	Dirección	10.21.5.99	Reply from 10.21.5.99: bytes=32 time=3ms TTL=254
	S2, VLAN 4	IPv6	2001:db5:acad:c: :99	Reply from 2001:db5:acad:c: :99: bytes=32 time=2ms TTL=254
	PC-B	Dirección	10.21.5.53	Reply from 10.21.5.53: bytes=32 time=2ms TTL=254
	PC-B	IPv6	2001:db5:acad:b::50	Reply from 2001:db5:acad:b::50: bytes=32 time=2ms TTL=254
	R1 Bucle 0	Dirección	209.165.201.1	Reply from 209.165.201.1: bytes=32 time=6ms TTL=255
	R1 Bucle 0	IPv6	2001:db5:acad:209::1	Reply from 2001:db5:acad:209::1: bytes=32 time<1ms TTL=255
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Reply from 10.19.8.98: bytes=32 time=2ms TTL=254
	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Reply from 2001:DB8:ACAD:209::1: bytes=32 time=12ms TTL=255
	R1, G0/0/1.2	Dirección	10.21.5.1	Reply from 10.21.5.1: bytes=32 time=2ms TTL=254
	R1, G0/0/1.2	IPv6	2001:db5:acad:a::1	Reply from 2001:db5:acad:a: :1: bytes=32 time<1ms TTL=255
	R1, G0/0/1.3	Dirección	10.21.5.65	Reply from 10.21.5.65: bytes=32 time=2ms TTL=254
	R1, G0/0/1.3	IPv6	2001:db5:acad:b: :1	Reply from 2001:db5:acad:b: :1: bytes=32 time<1ms TTL=255
	R1, G0/0/1.4	Dirección	10.21.5.97	Reply from 10.21.5.97: bytes=32 time=2ms TTL=254
	R1, G0/0/1.4	IPv6	2001:db5:acad:c::1	Reply from 2001:db5:acad:c::1: bytes=32 time<1ms TTL=255

	S1, VLAN 4	Dirección	10.21.5.98	Reply from 10.21.5.98: bytes=32 time=2ms TTL=254
	S1, VLAN 4	IPv6	2001:db5:acad:c::98	Reply from 2001:db5:acad:c: :98: bytes=32 time=2ms TTL=254
	S2, VLAN 4	Dirección	10.21.5.99	Reply from 10.21.5.99: bytes=32 time=2ms TTL=254
	S2, VLAN 4	IPv6	2001:db5:acad:c: :99	Reply from 2001:db5:acad:c: :99: bytes=32 time=2ms TTL=254

Tabla 11 Verificación de conectividad de extremo a extremo

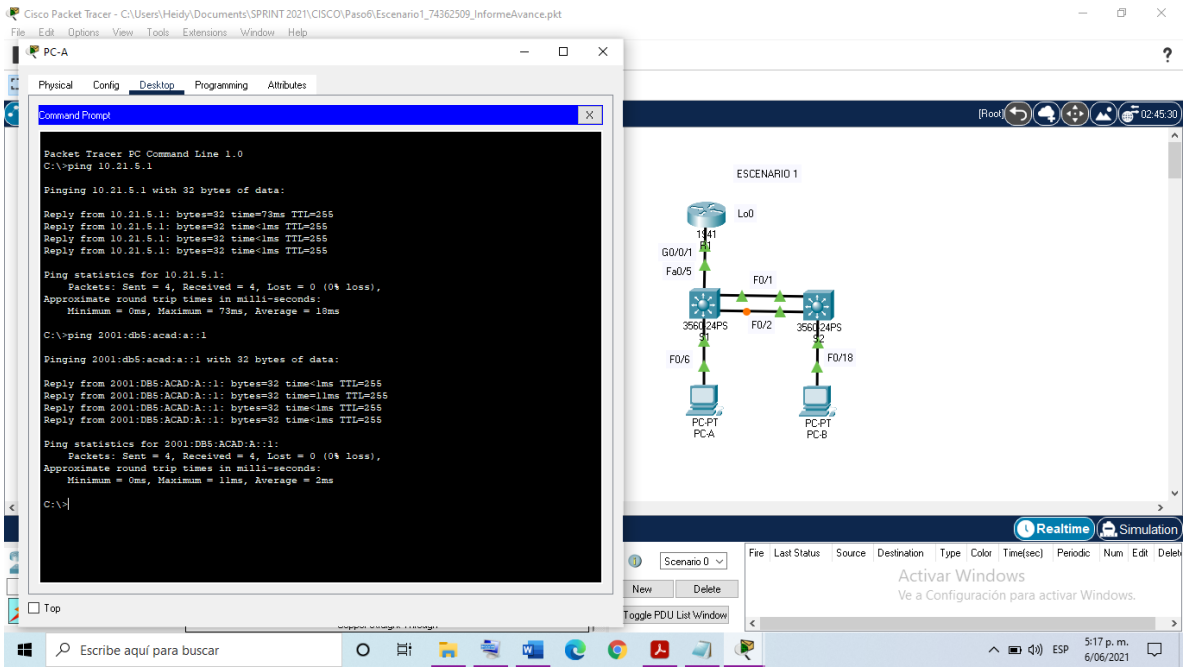

Figura 5 Verificación de conectividad en PC-A a R1 G0/0/1.2. Fuente: propia

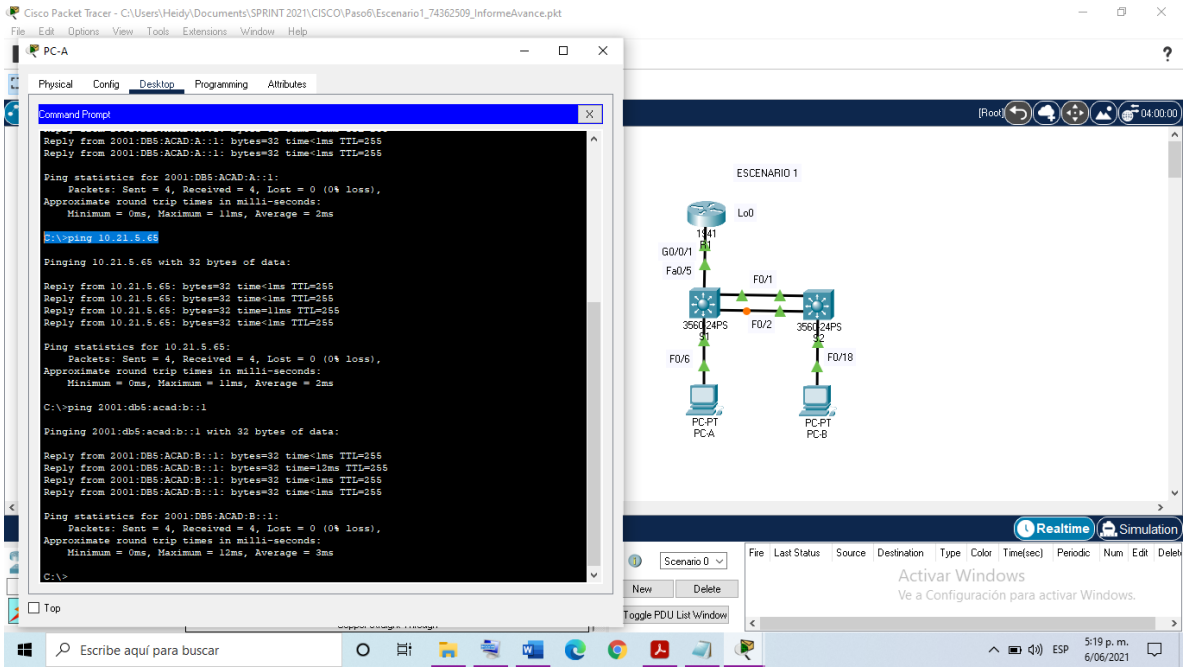

Figura 6 Verificación de conectividad en PC-A a R1 G0/0/1.3. Fuente: propia

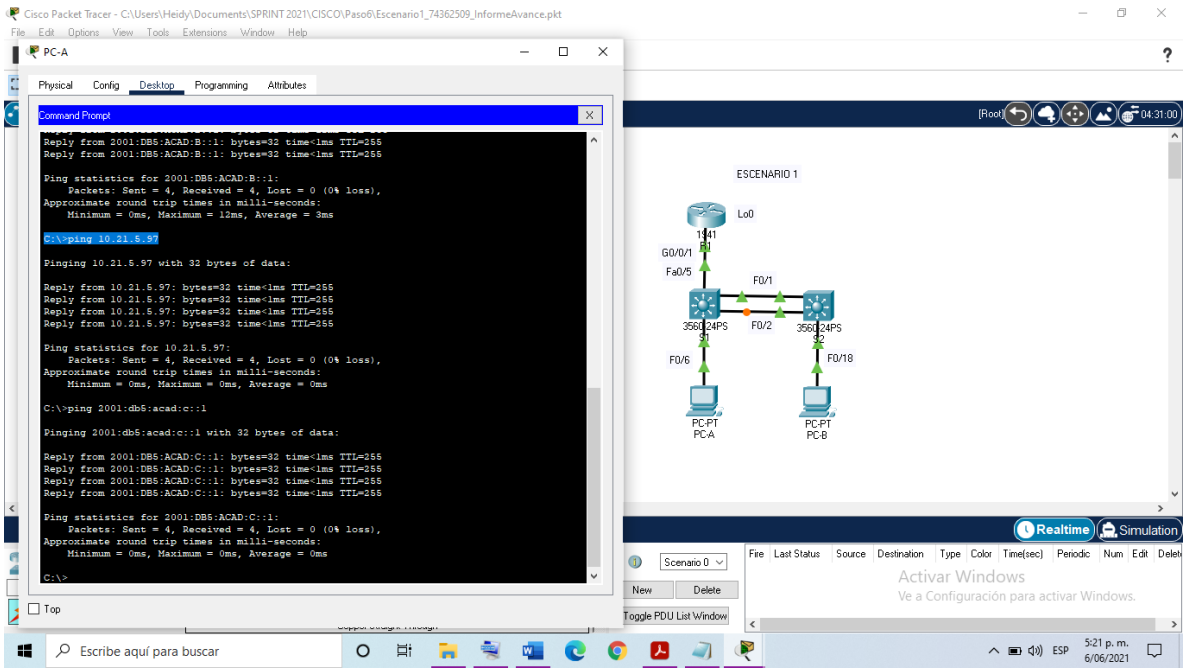

Figura 7 Verificación de conectividad en PC-A a R1 G0/0/1.4. Fuente: propia

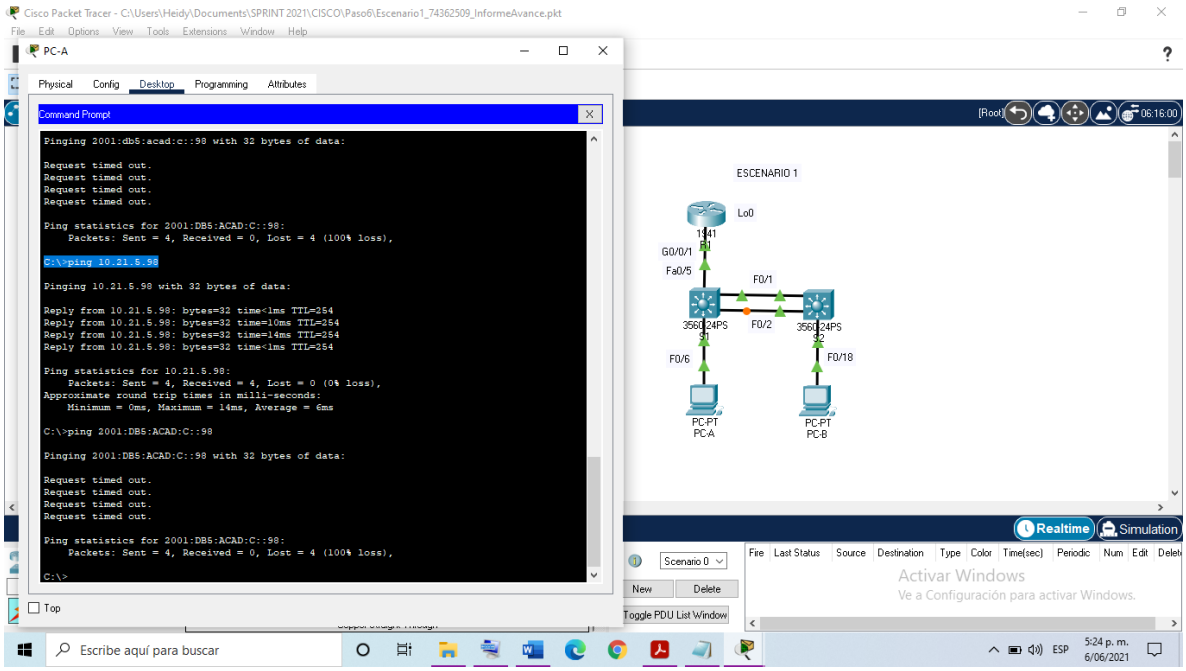

Figura 8 Verificación de conectividad en PC-A a S1 VLAN 4. Fuente: propia

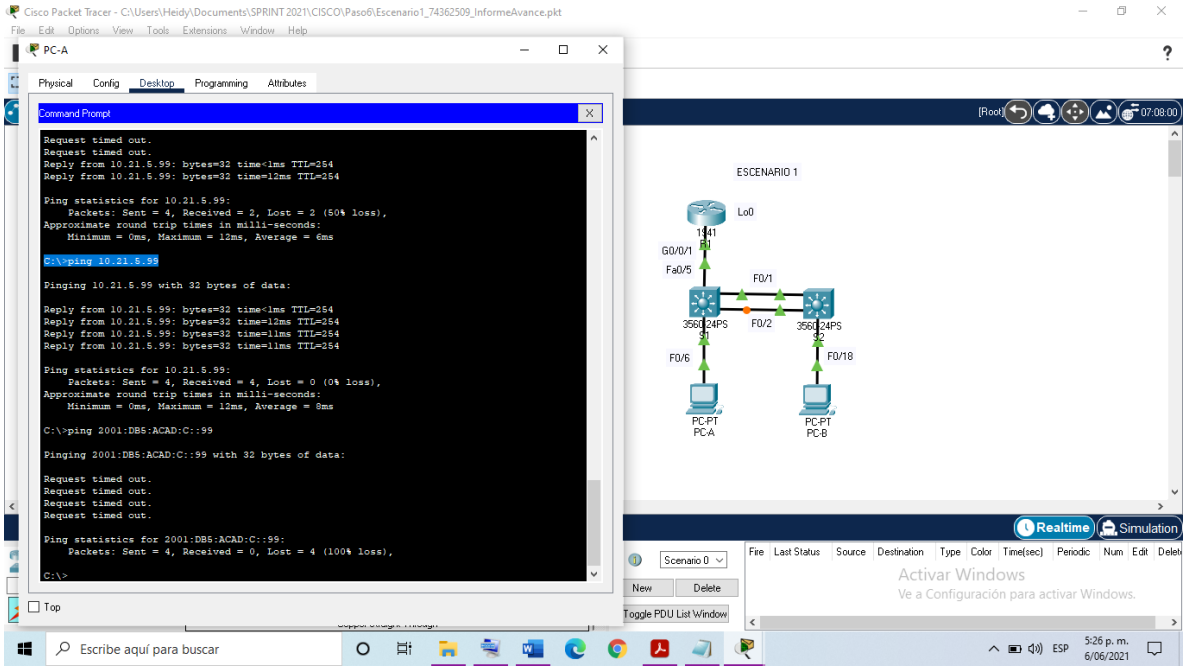

Figura 9 Verificación de conectividad en PC-A a S2 VLAN 4. Fuente: propia

3.1 ESCENARIO 2

Se configura 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

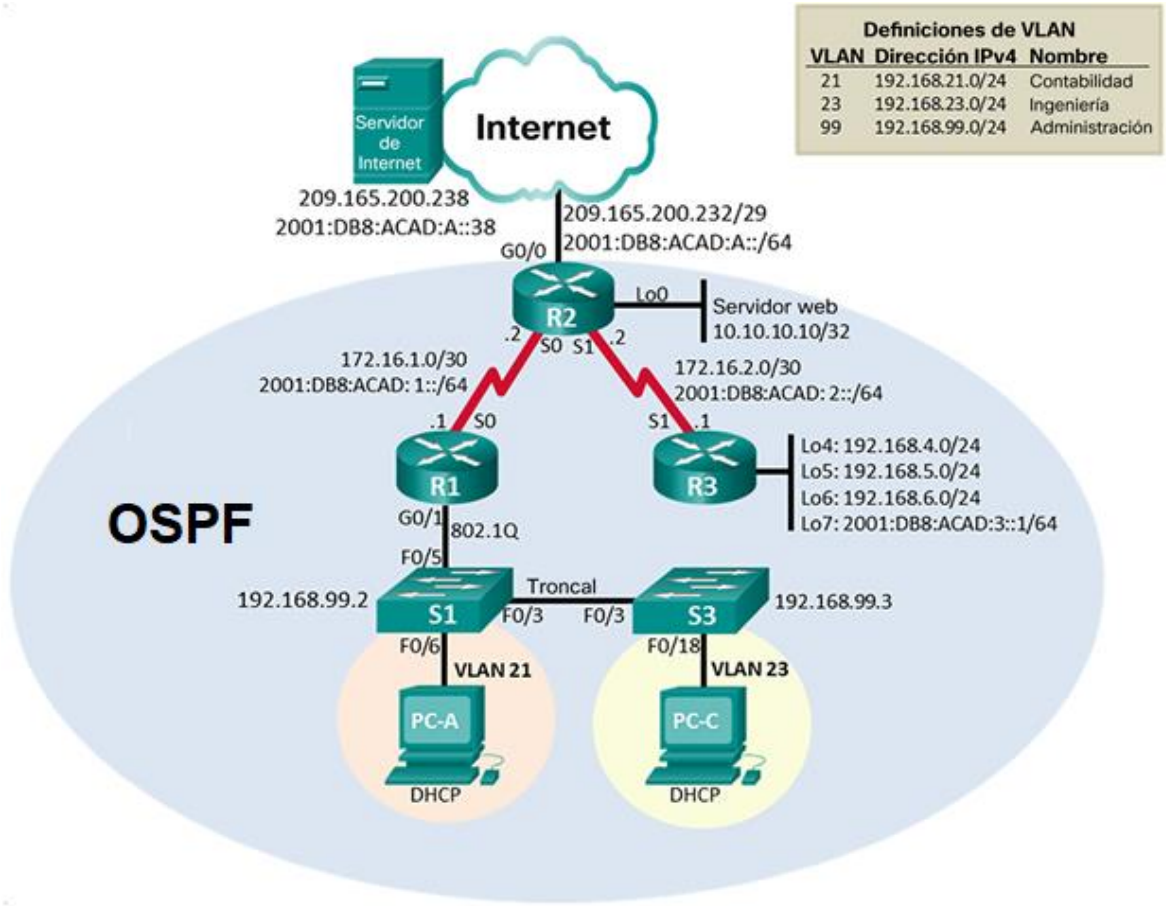

Figura 10 Topología del segundo escenario. Fuente: cisco

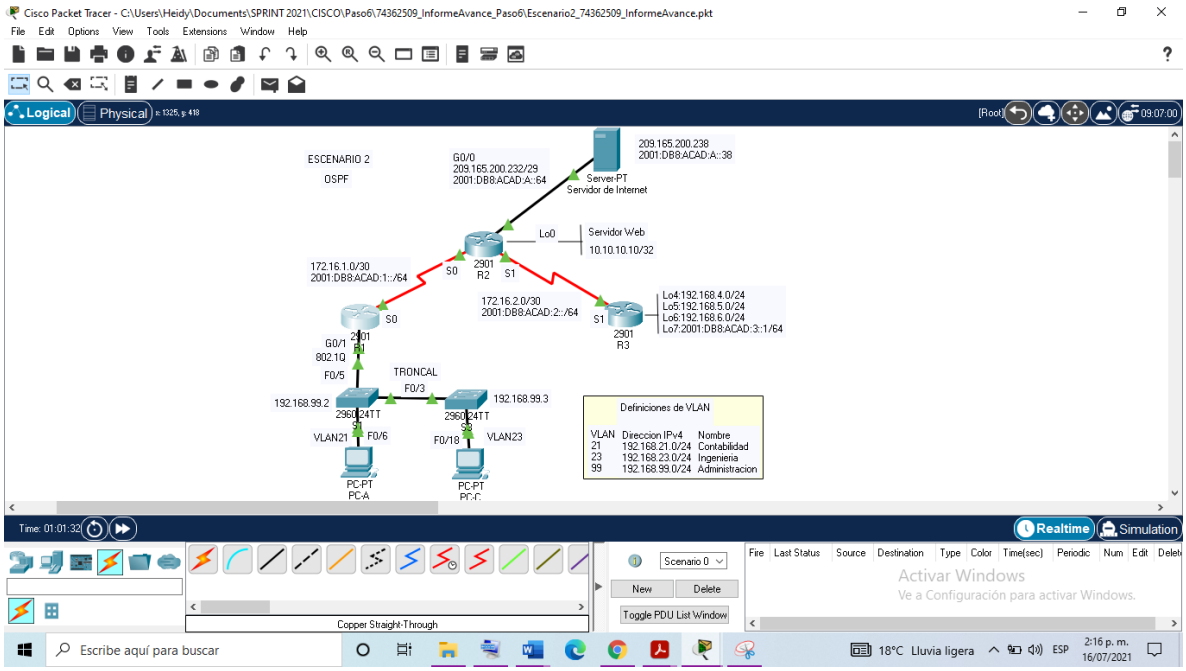

Figura 11 Escenario 2 en el software cisco packet tarcer. Fuente: propia

PARTE 1: INICIALIZAR DISPOSITIVOS

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos y por medio de los siguientes comandos.se realizan las configuraciones de formateo y reinicio tanto en los Routers como en los Switch.

Ingresamos a cada dispositivo dando doble clic y a través de la ventana (CLI), ingresamos el comando enable, que permite cambiar el modo EXEC del usuario al modo EXEC privilegiado donde si podemos realizar las configuraciones del dispositivo, luego ingresamos el comando erase startup-config para eliminar el contenido de la NVRAM y por último ingresamos el comando reload para reiniciar el dispositivo.

Tarea	Comando de ios
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Continue? [confirm] [Enter] [OK] Erase of nvram: complete
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] [Enter]
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] [Enter] [OK] Erase of nvram: complete Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] [Enter]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show vlan brief

Tabla 12 Inicialización de los routers y switchs

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

En la siguiente tabla, se encuentran las direcciones IPv4 e IPv6 correspondientes a la computadora de internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 13 Direcciones IPv4 e IPv6 para configurar en la computadora

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	R1(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 console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)n#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	R1(config)#interface s0/3/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config)#interface s0/3/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0 R1(config)#ipv6 route ::/0 serial s0/3/0

Tabla 14 Configuraciones básicas de R1

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	R2(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config-line)#enable secret class
Contraseña de acceso a la consola	R2(config)# line console 0 R2(config)#password cisco R2(config-line)# login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config)#password cisco R2(config-line)# login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	R2(config)#interface s0/3/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config)#interface s0/3/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#interface s0/3/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#clock rate 12800 R2(config-if)#no shutdown R2(config)#interface s0/3/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	R2(config)#interface g0/0 R2(config)# description Conexion Servidor R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown R2(config)#interface g0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown
Ruta predeterminada	R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:2::1 R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)# ipv6 route ::/0 2001:BD8:ACAD:A::38

Tabla 15 Configuraciones básicas en R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R3(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 console 0 R3(config)#password cisco R3(config-line)# login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config)#password cisco

	R3(config-line)# login
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 s0/3/1 R3(config)# description Conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config)#interface s0/3/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown

Interfaz loopback 4	R3(config)#interface loopback 4
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 4)
	R3(config-if)#ip address 192.168.4.0 255.255.255.0
	R3(config-if)#no shutdown

Interfaz loopback 5	R3(config)#interface loopback 5
	R3(config)# description Interfaz virtual (para pruebas, en este caso el 5)
	R3(config-if)#ip address 192.168.5.0 255.255.255.0
	R3(config-if)#no shutdown

Interfaz loopback 6	R3(config)#interface loopback 6
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 6)
	R3(config-if)#ip address 192.168.6.0 255.255.255.0
	R3(config-if)#no shutdown

Interfaz loopback 7	R3(config)#interface loopback 7
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 7)
	R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
	R3(config-if)#no shutdown

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2

Tabla 16 Configuraciones básicas de R3

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S1(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 console 0 S1(config)#password cisco S1(config-line)# login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config)#password cisco S1(config-line)# login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado$

Tabla 17 Configuraciones básicas de S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(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 console 0 S3(config)#password cisco S3(config-line)# login
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config)#password cisco S3(config-line)# login

Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$

Tabla 18 Configuraciones básicas de S3

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	R1#ping 172.16.1.2 Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1 Success rate is 100 percent(5/5) round-trip min/avg/max = 1/2/8 ms
PC de Internet	Gateway predeterminado	209.165.200.233	>ping 209.165.200.233 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Tabla 19 Verificación de conectividad de la red

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

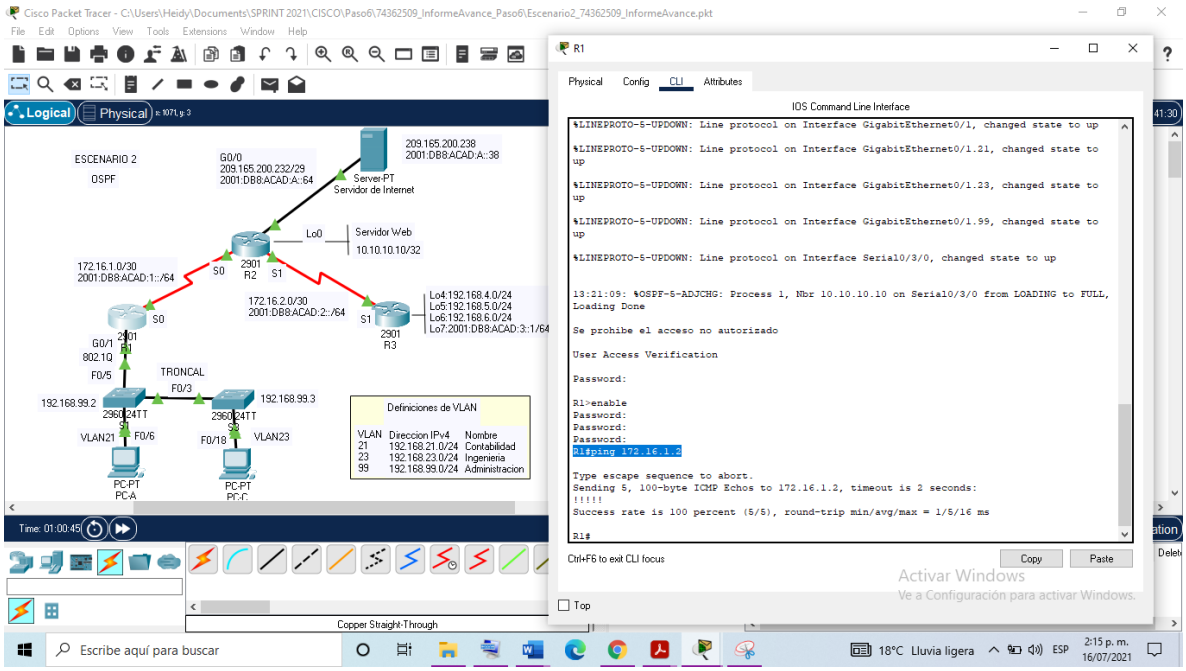

Figura 12 Verificación de conectividad desde R1 a R2. Fuente: propia

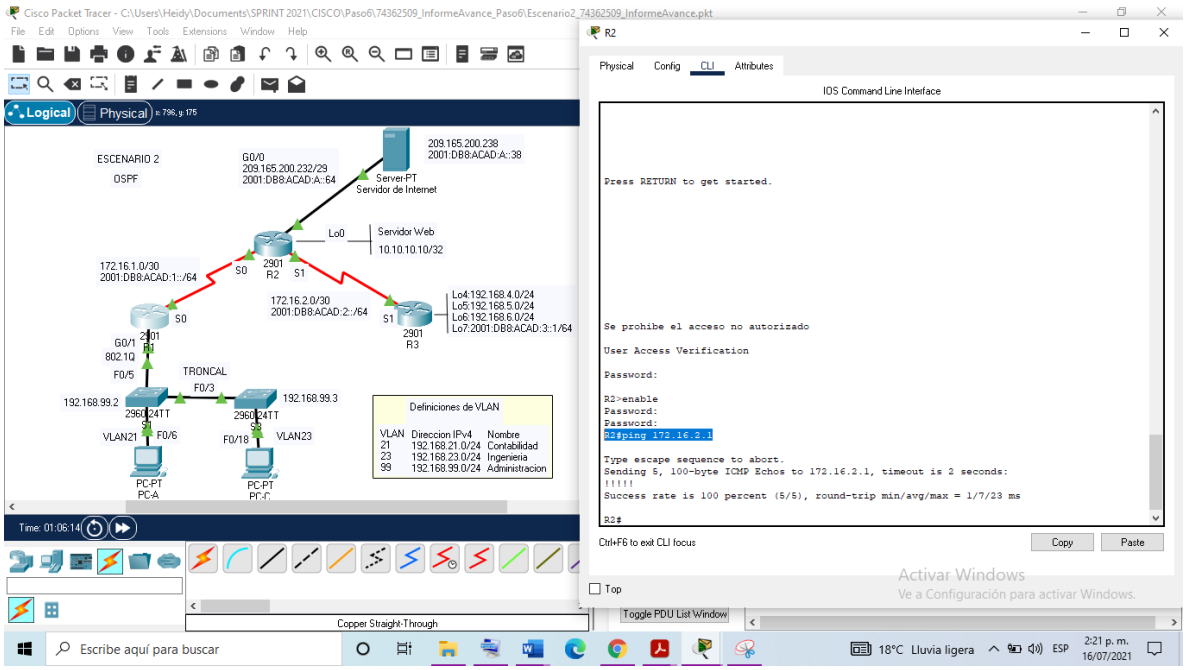

Figura 13 Verificación de conectividad desde R2 a R3. Fuente: propia

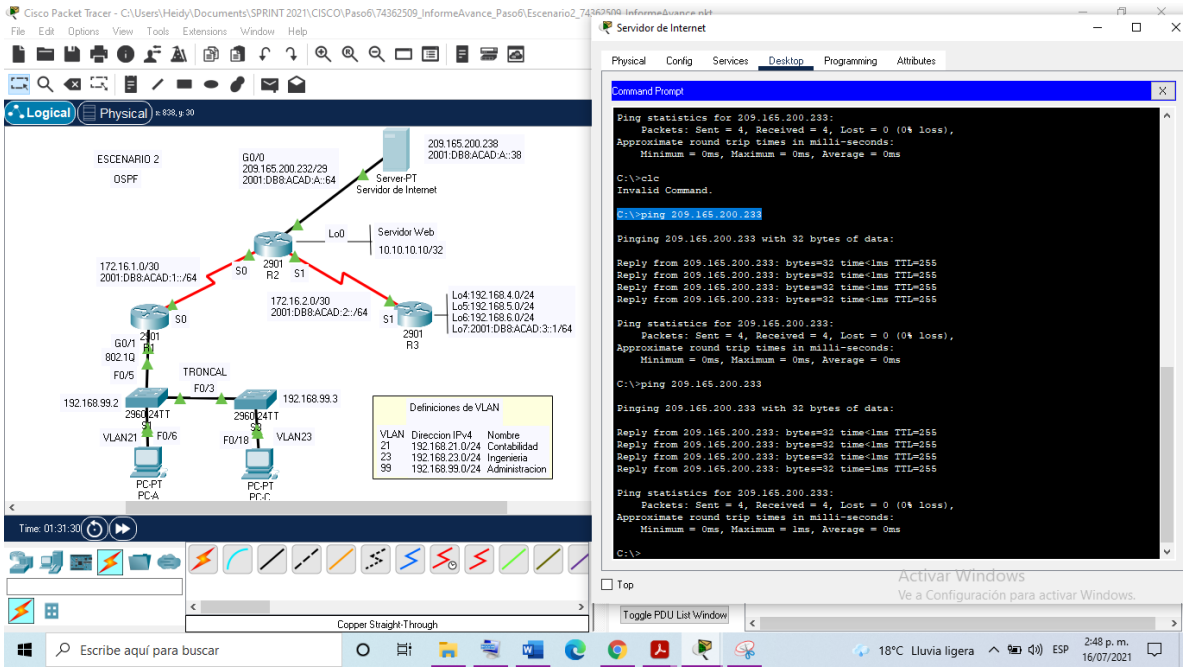

Figura 14 Verificación de conectividad desde PC de Internet a Gateway. Fuente: propia

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:

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 ingeniería S1(config-vlan)#vlan 99 S1(config-vlan)#name administración S1(config-vlan)#exit
Asignar la dirección IP de administración.	S1(config-if)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway	S1(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-rangen)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 20 Configuración de la seguridad entre las vlan de S1.

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	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 administración 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 fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S3(config-if)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if)#interface fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if-range)#no shutdown
Apagar todos los puertos sin usar	S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 21 Configuración de la seguridad entre las vlan de S3

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	R1(config)#interface g0/1.21 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config)#description LAN de contabilidad VLAN 21
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)# interface g0/1.23 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config)#description LAN de Ingeniería VLAN 23
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)# interface g0/1.99 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 99

	R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config)#description LAN de Administración VLAN 99
Activar la interfaz G0/1	R1(config-subif)# interface g0/1 R1(config-subif)#no shutdown

Tabla 22 Configuración de la seguridad entre las vlan de R1.

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1 y 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	S1#ping 192.168.99.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 21)
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 22)
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 23)
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 24)

Tabla 23 Verificación de conectividad de la red

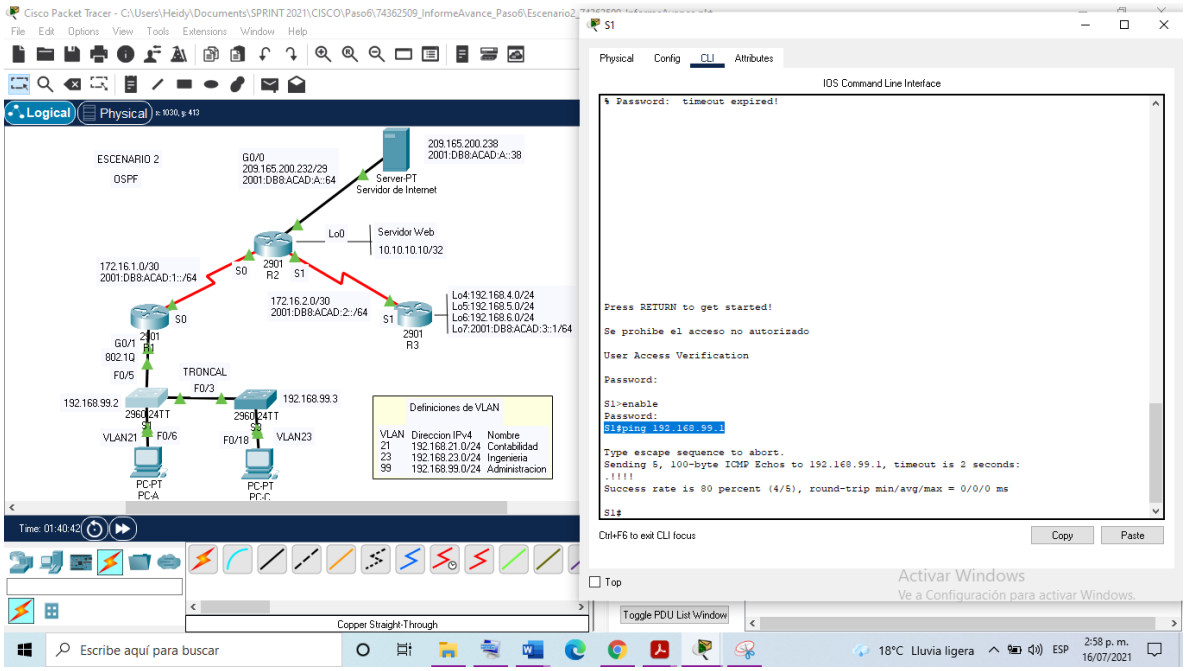

Figura 15 Verificación de conectividad desde S1 a R1 (VLAN99). Fuente: propia

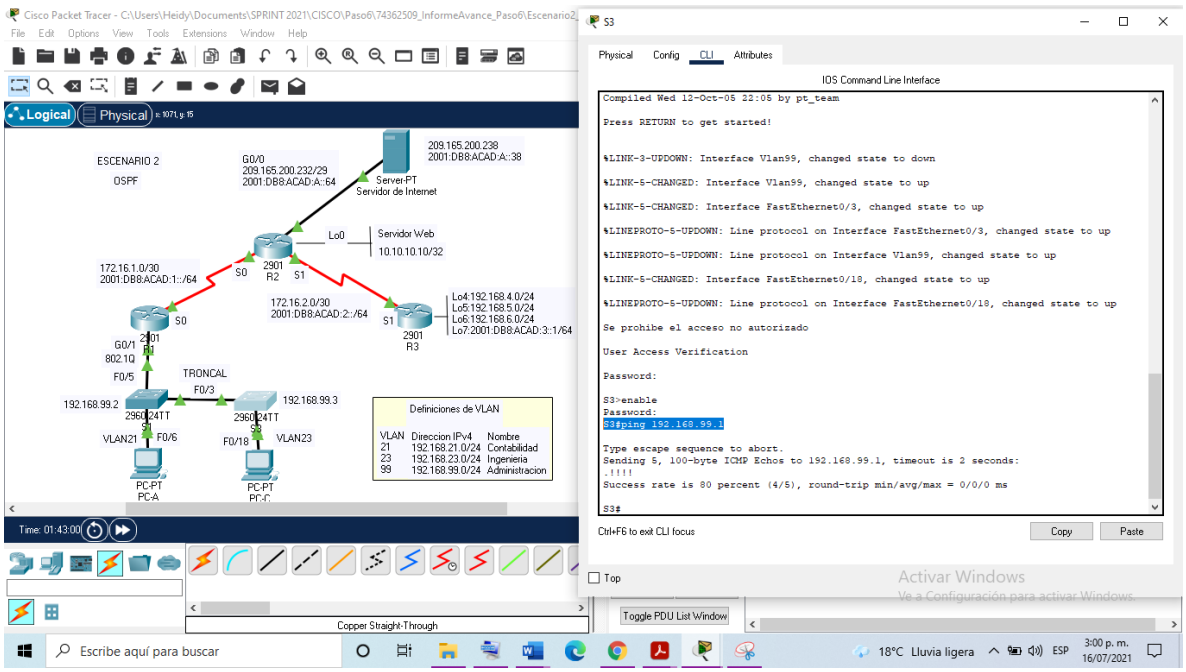

Figura 16 Verificación de conectividad desde S3 a R1 (VLAN99). Fuente: propia

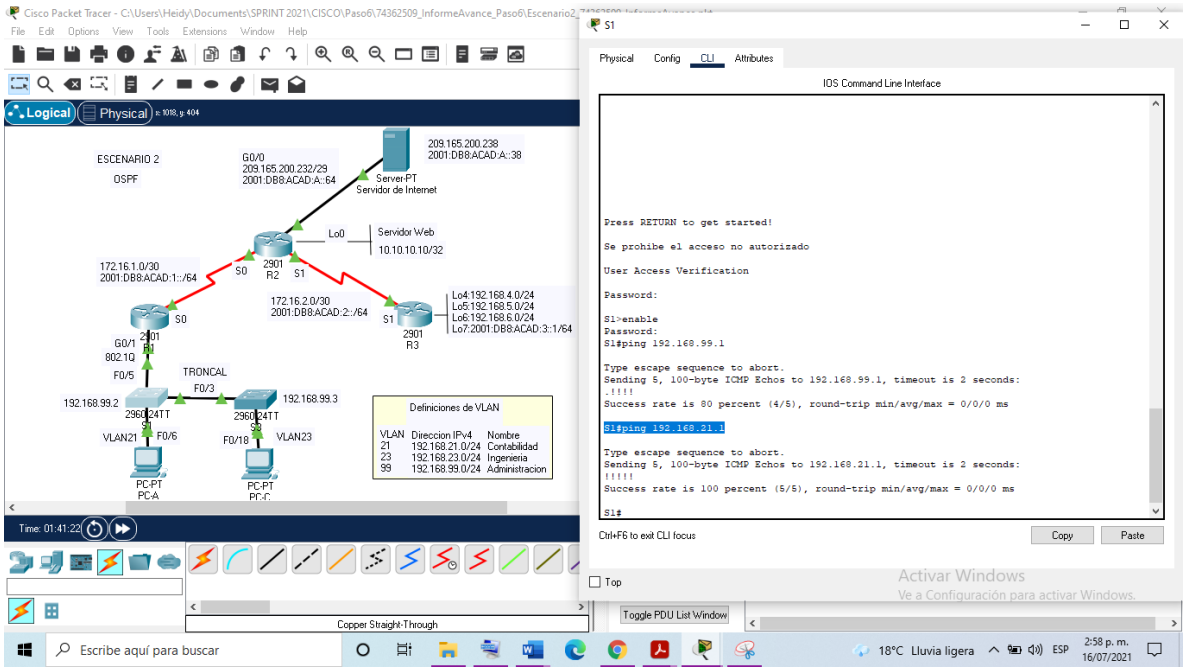

Figura 17 Verificación de conectividad desde S1 a R1 (VLAN21). Fuente: propia

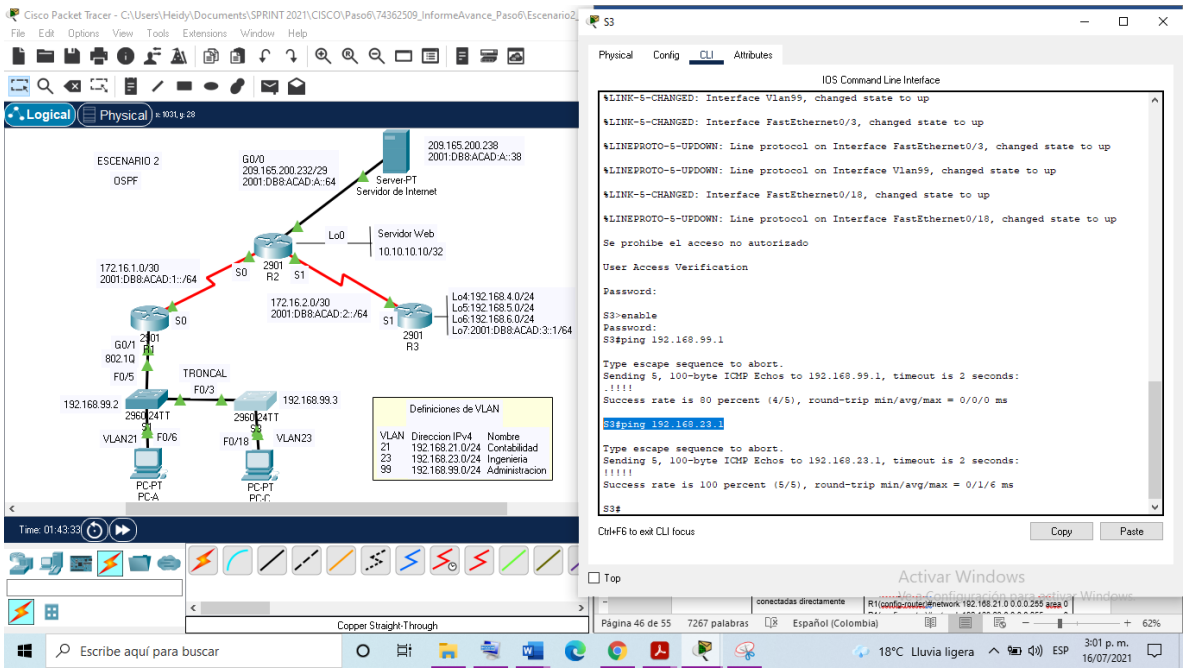

Figura 18 Verificación de conectividad desde S3 a R1 (VLAN21). Fuente: propia

Paso 5: Habilitar el envío de tráfico IPv6 en R1, R2 y R3.

Por defecto, IPv6 está desactivado en un dispositivo Cisco.

Elemento o tarea de configuración	Especificación
Habilitar el routing de unidifusión IPv6 en R1, R2 y R3.	R1#**configure terminal** R1(config)#**ipv6 unicast-routing** R1(config)#**exit** R2# **configure terminal** R2(config)#**ipv6 unicast-routing** R2(config)#**exit** R3# **configure terminal** R3(config)#**ipv6 unicast-routing** R3(config)#**exit**

Tabla 24 Habilitación tráfico IPv6 en R1, R2 y R3.

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 area 0	R1(config)#router ospf 1 R1(config)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.255 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 g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 25 Configuración OSPF en el R1.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF area 0	R2(config)#router ospf 1 R2(config)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 192.168.4.0 0.0.0.255 area 0 R2(config-router)#network 192.168.5.0 0.0.0.255 area 0 R2(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 26 Configuración OSPF en el R2.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas

Elemento o tarea de configuración	Especificación
Configurar OSPF area 0	R3(config)#router ospf 1 R3(config)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.255 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 R3(config-router)#passive-interface lo7

Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 27 Configuración OSPF en el R3

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?	R1#Show ip protocols R2#Show ip protocols R3#Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#Show ip route ospf R2#Show ip route ospf R3#Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#Show run-config | section router ospf R2#Show run-config | section router ospf R3#Show run-config | section router ospf

Tabla 28 Verificar la información de OSPF

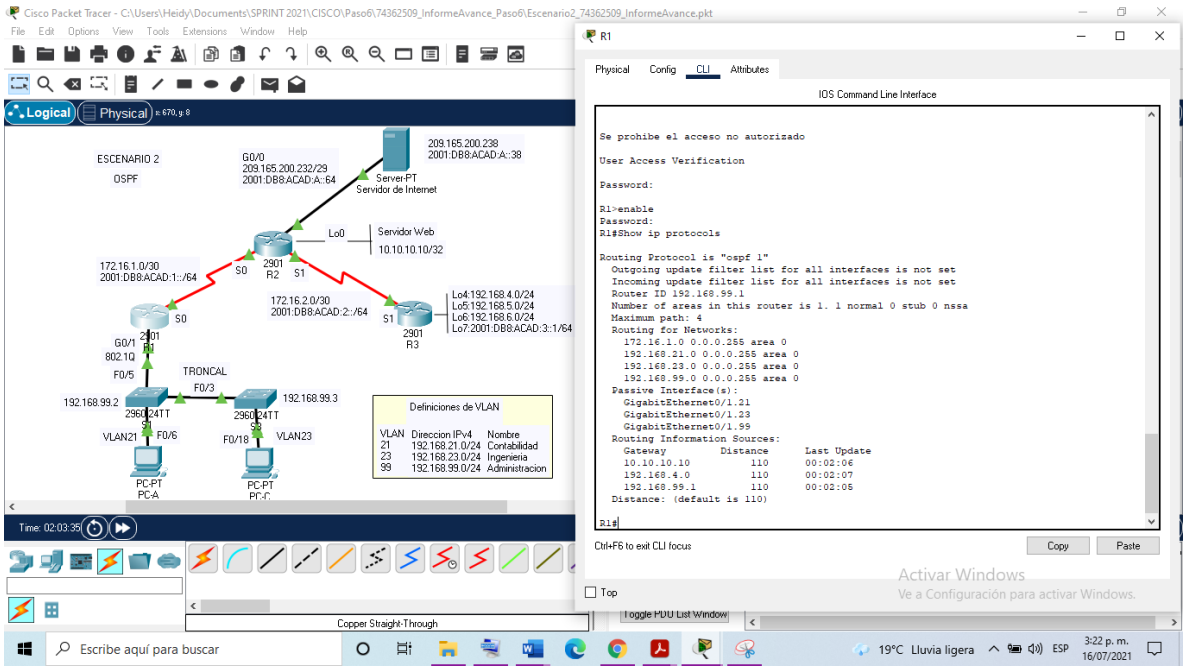

Figura 19 Comando show ip protocols en R1. Fuente: propia

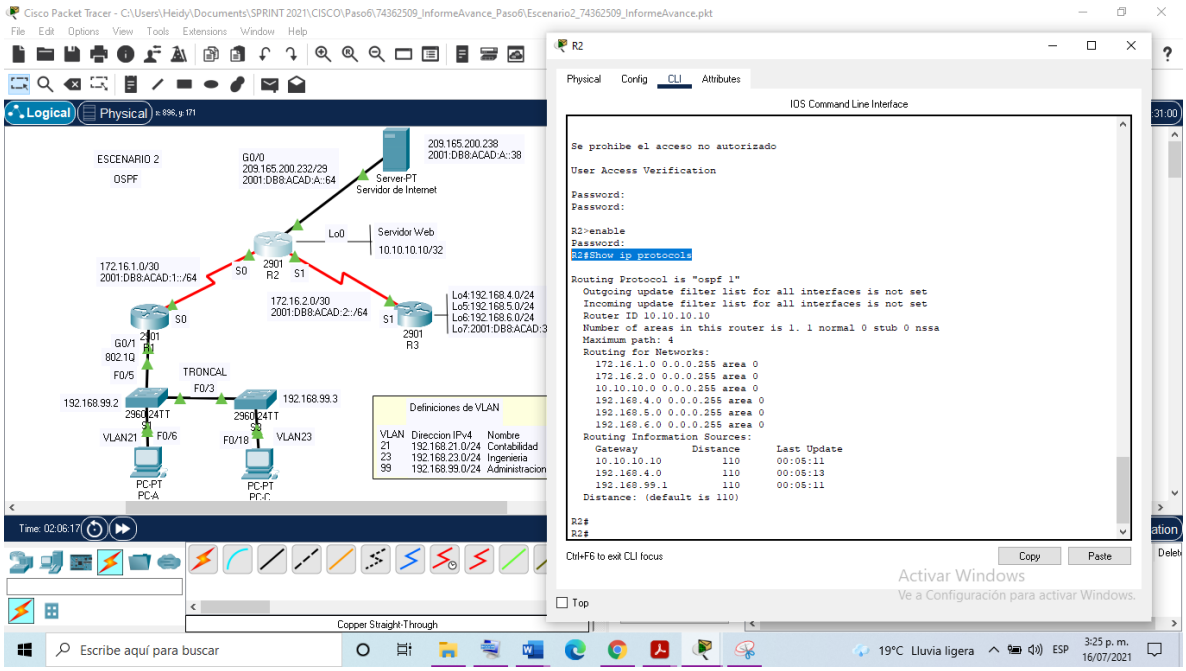

Figura 20 Comando show ip protocols en R2. Fuente: propia

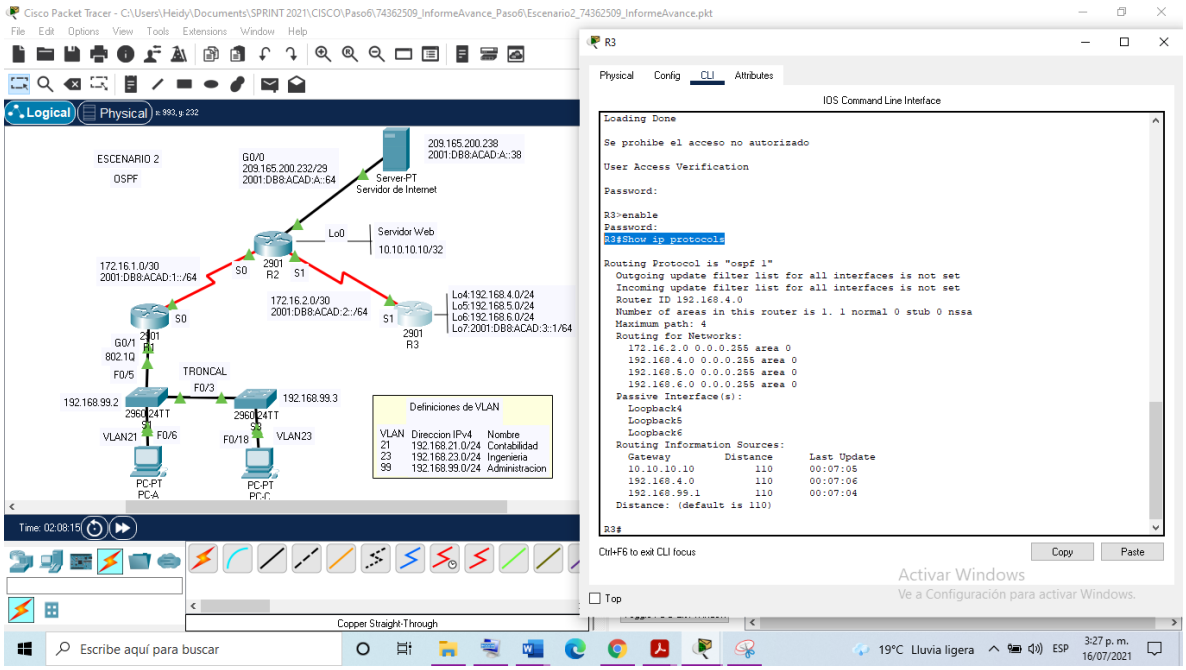

Figura 21 Comando show ip protocols en R3. Fuente: propia

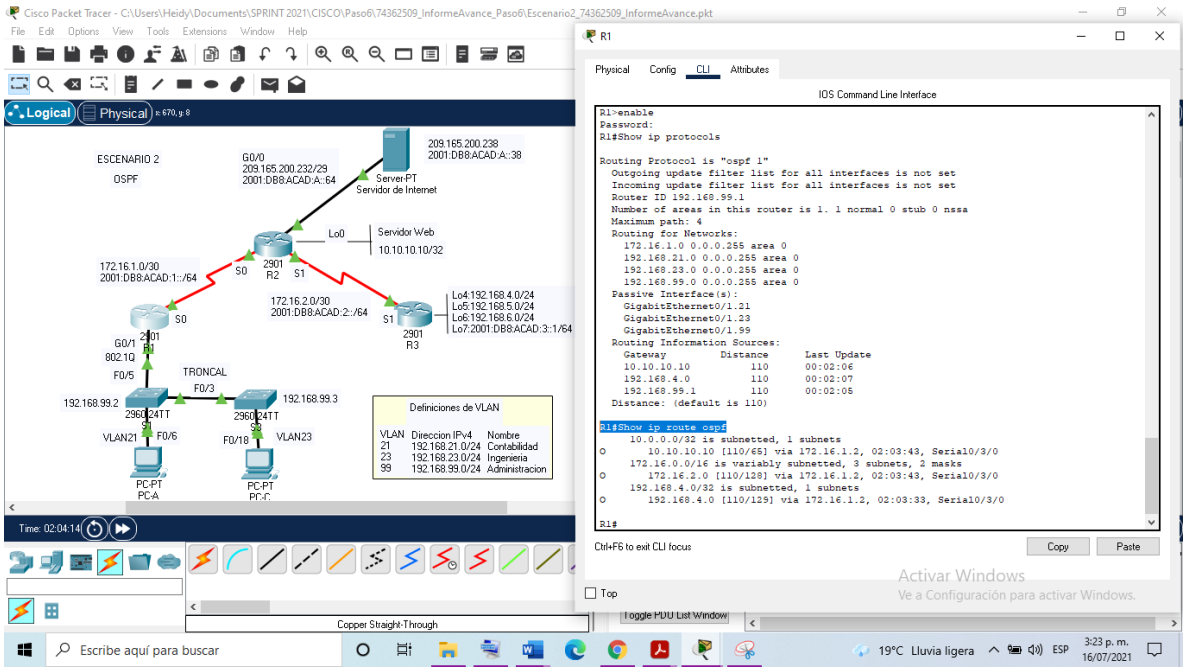

Figura 22 Comando show ip route ospf en R1. Fuente: propia

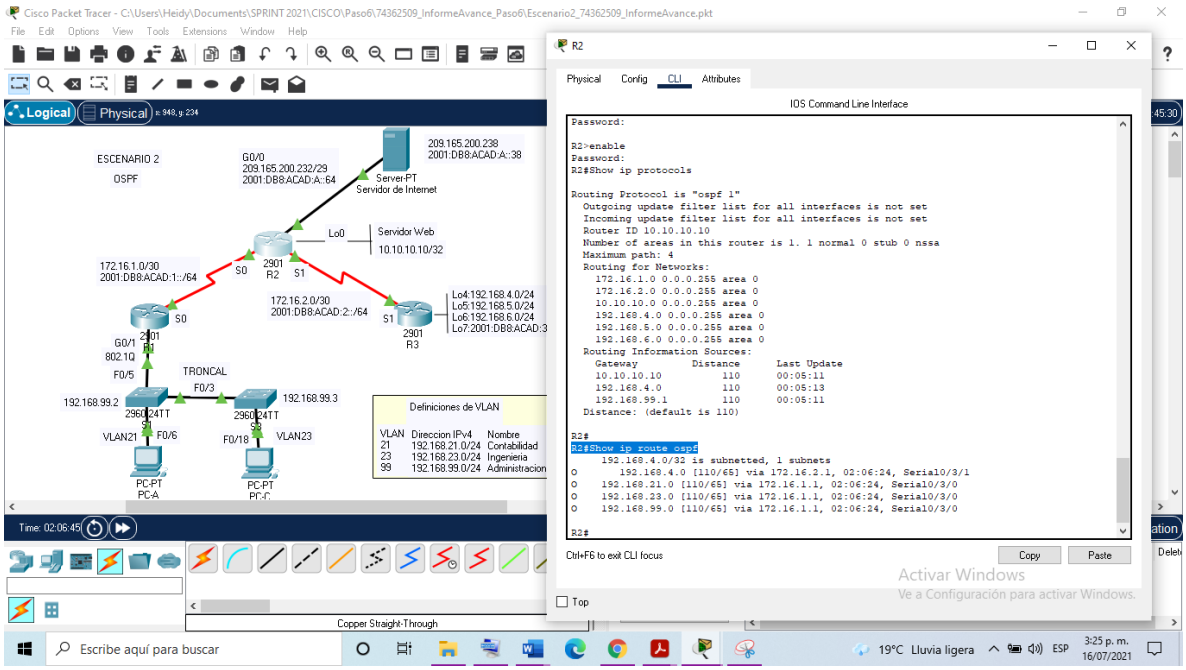

Figura 23 Comando show ip route ospf en R2. Fuente: propia

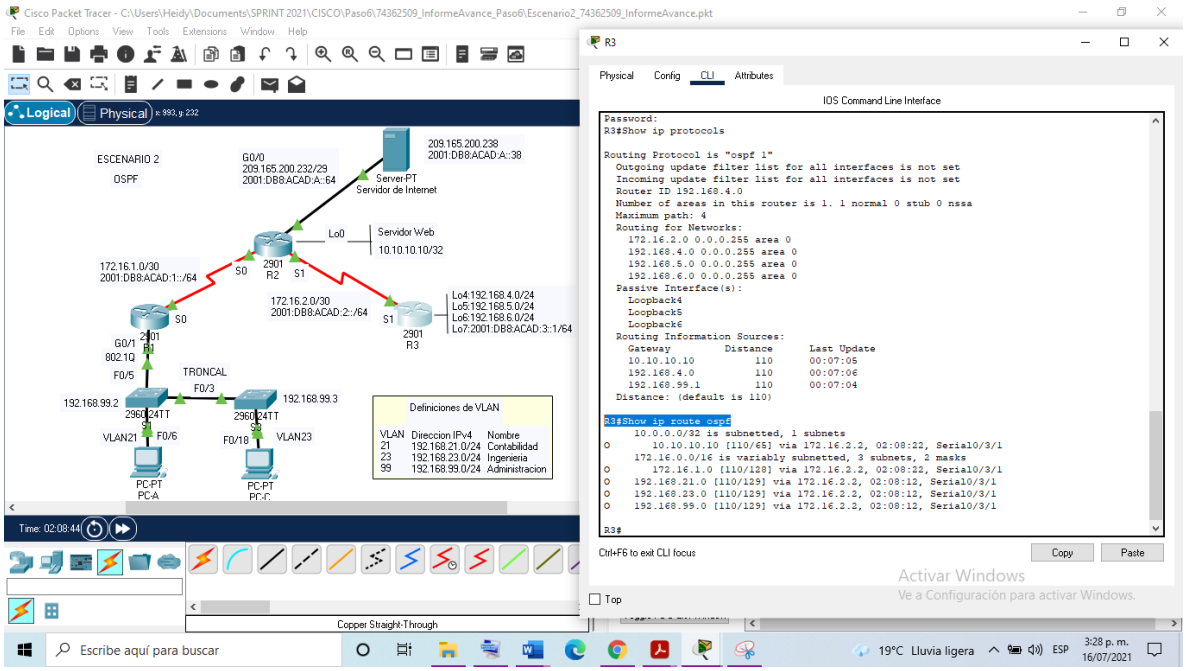

Figura 24 Comando show ip route ospf en R3. Fuente: propia

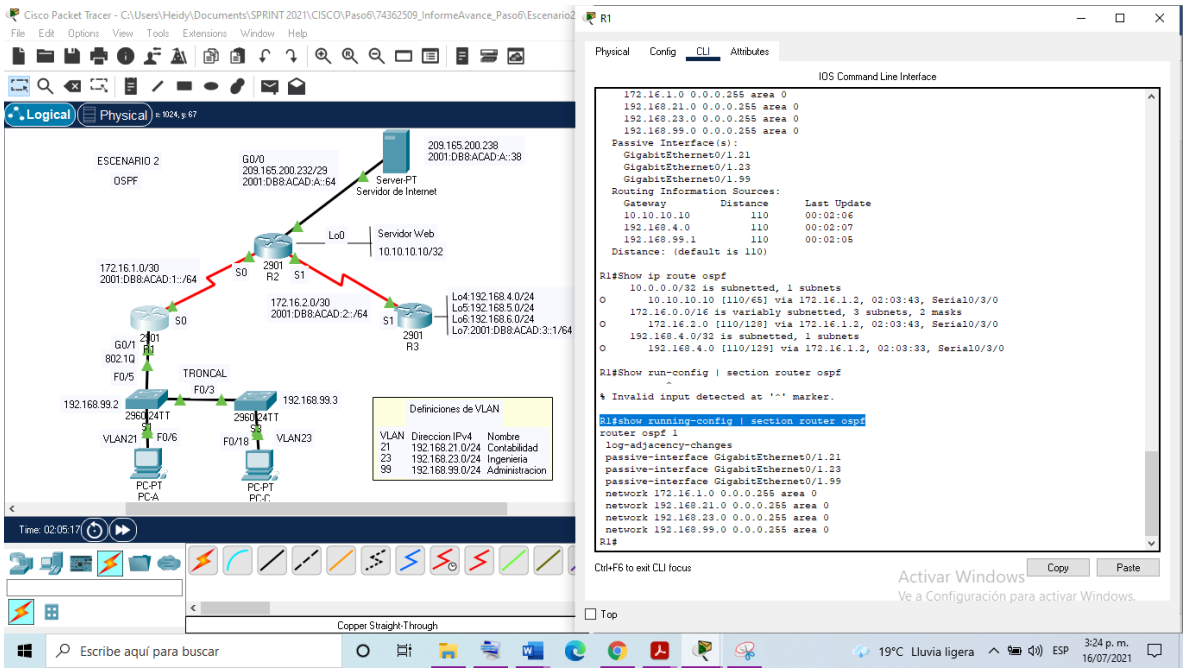

Figura 25 Comando show run-config | section router ospf en R1. Fuente: propia

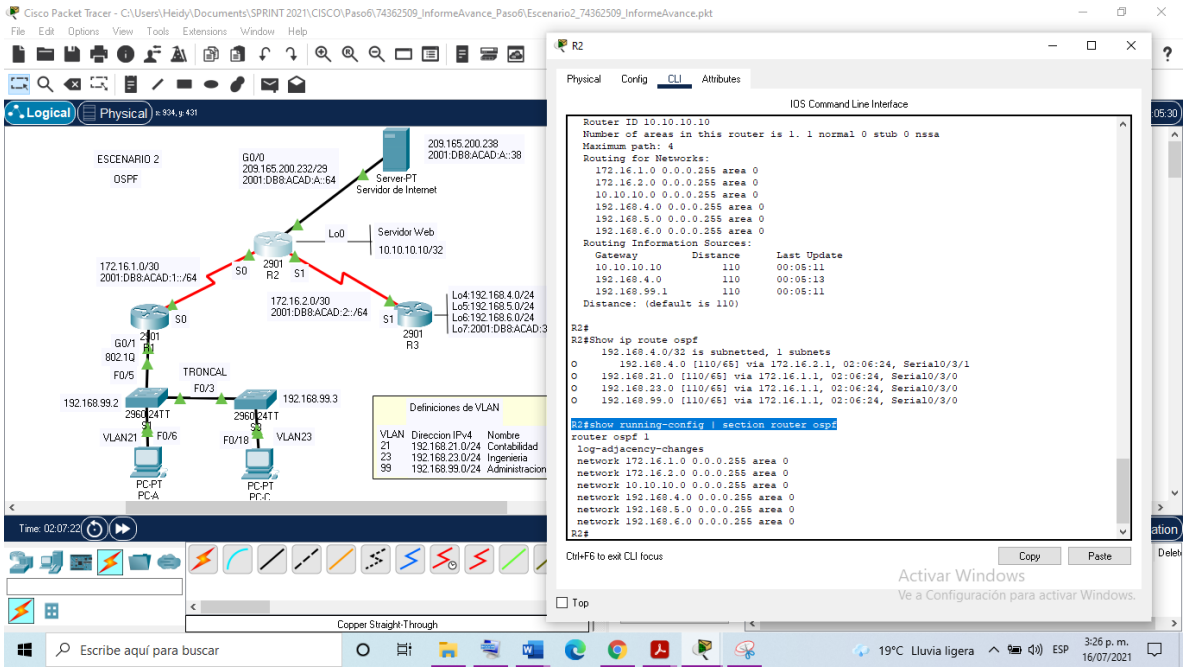

Figura 26 Comando show run-config | section router ospf en R2. Fuente: propia

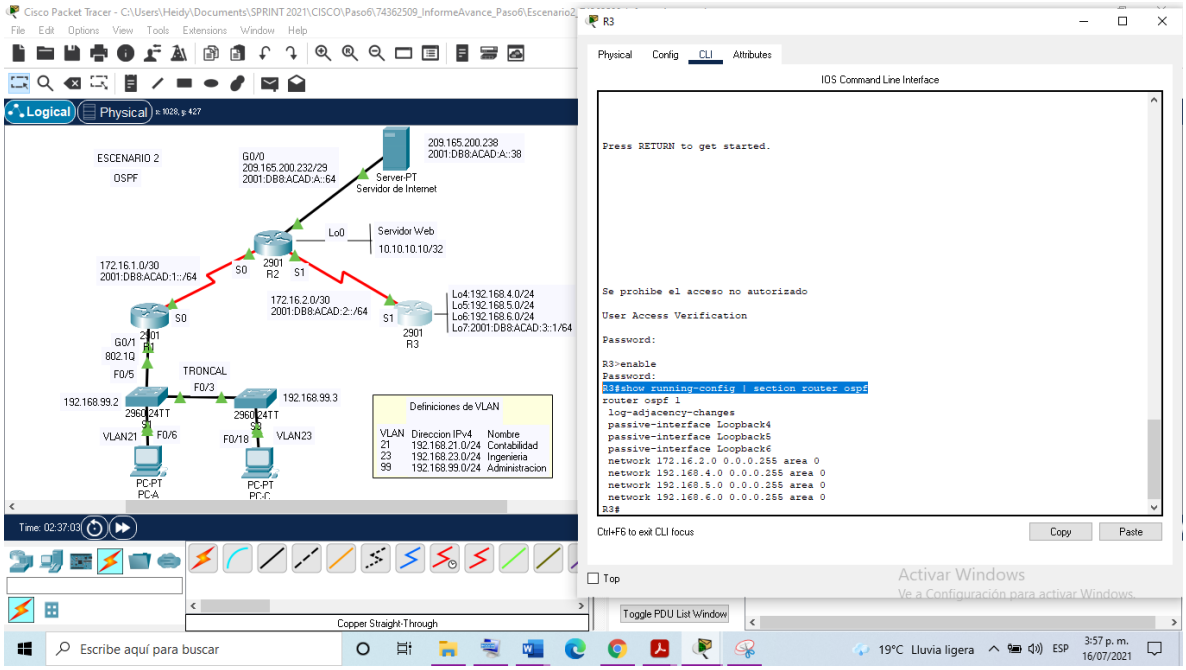

Figura 27 Comando show run-config | section router ospf en R3. Fuente: propia

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(config)#network 192.168.21.0 255.255.255.0 R1(config)#default-router 192.168.21.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(config)#network 192.168.23.0 255.255.255.0 R1(config)#default-router 192.168.23.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com

Tabla 29 Configuración de R1 como servidor de DHCP para IPV4

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	R2(config)#username webuser privilege 15 R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet Tracer no procesa la configuraion HTTP R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local

Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/1 R2(config)#ip nat outside R2(config)#interface fa0/6 R2(config)#ip nat inside R2(config)#interface loopback 0 R2(config)#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 0.0.3.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Tabla 30 Configuración NAT en R2 para IPV4

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

Tabla 31 Verificación del protocolo DHCP y NAT estática

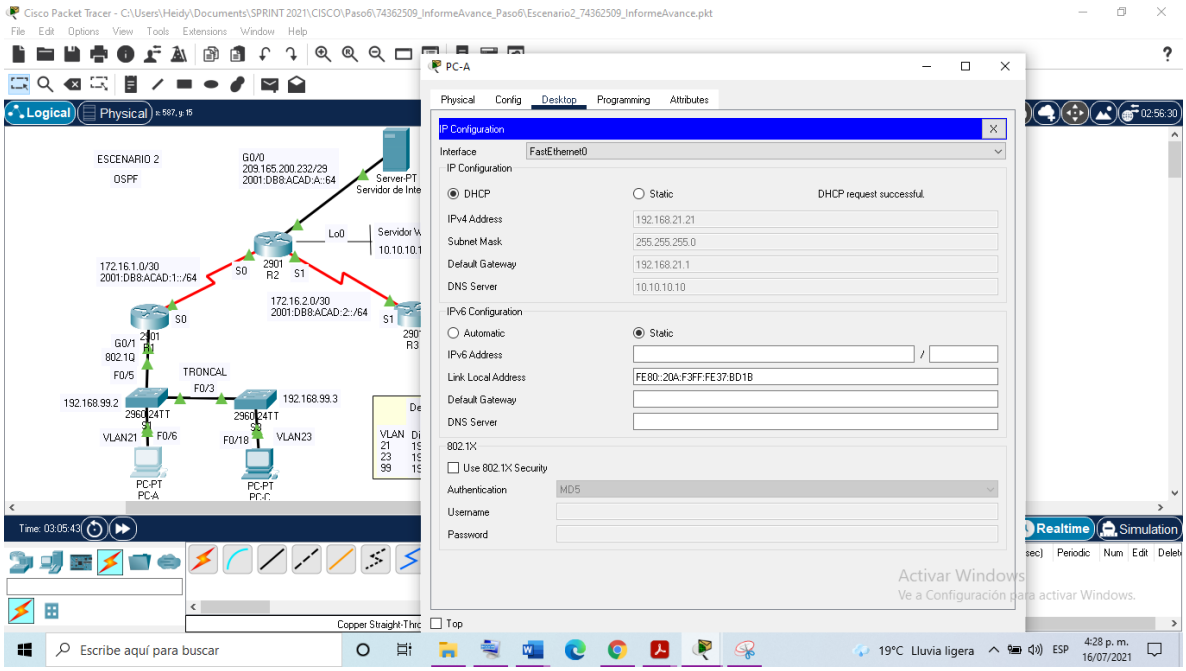

Figura 28 Verificación del protocolo DHCP en PC-A. Fuente: propia

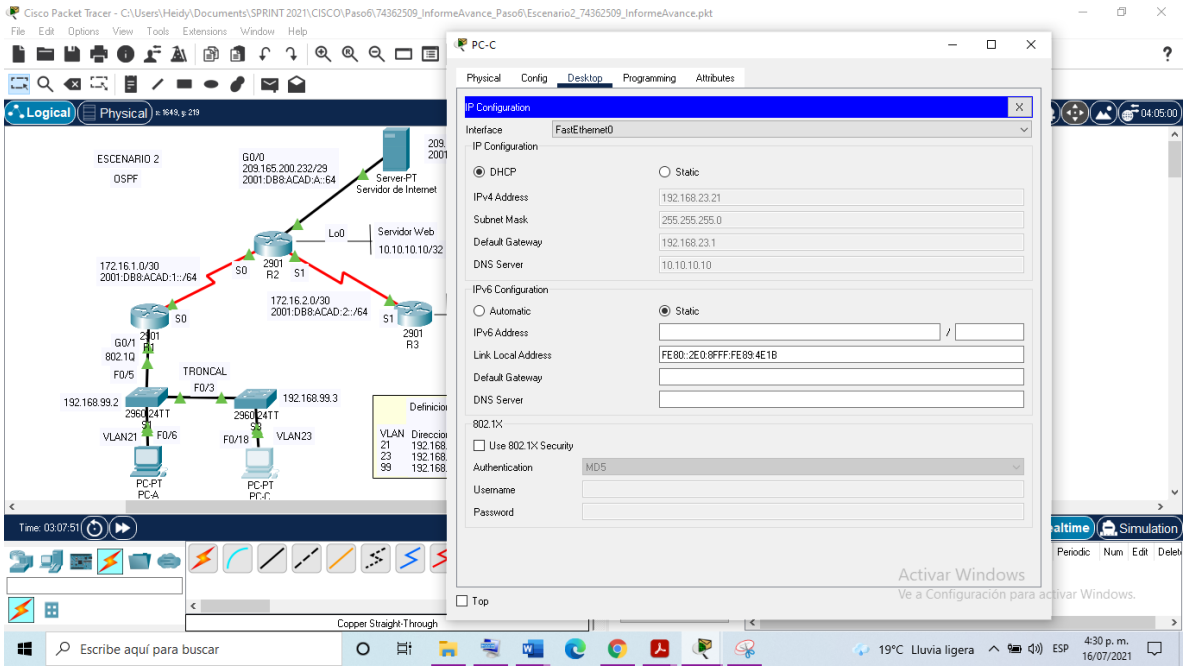

Figura 29 Verificación del protocolo DHCP en PC-B. Fuente: propia

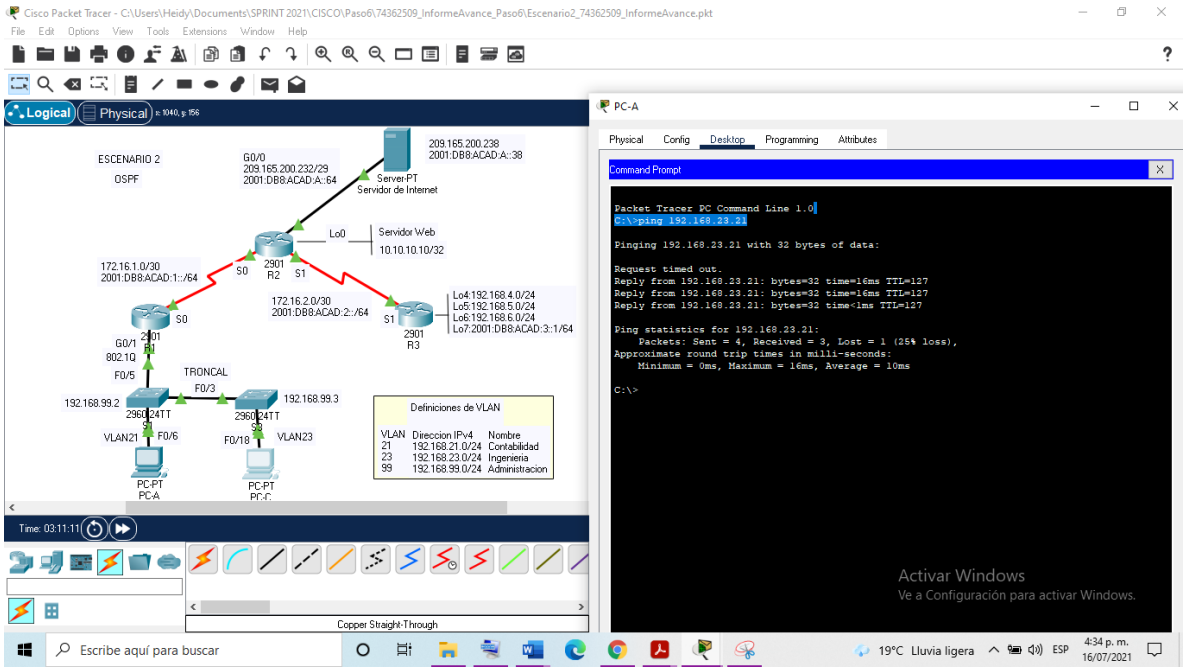

Figura 30 Verificación de conexión entre PC-A y PC-C. Fuente: propia

PARTE 6: CONFIGURAR NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 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.	R1#show ntp associations R1#show clock R1#show ntp status

Tabla 32 Configuración NTP

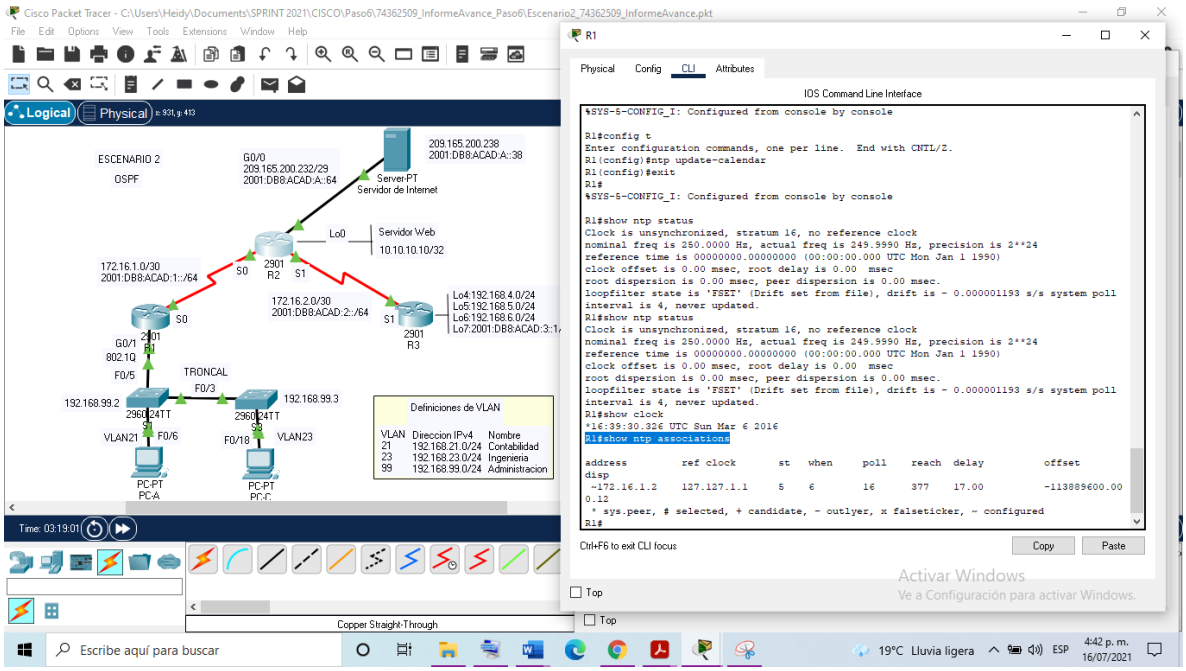

Figura 31 Verificación de la configuración NTP en R1. Fuente: propia

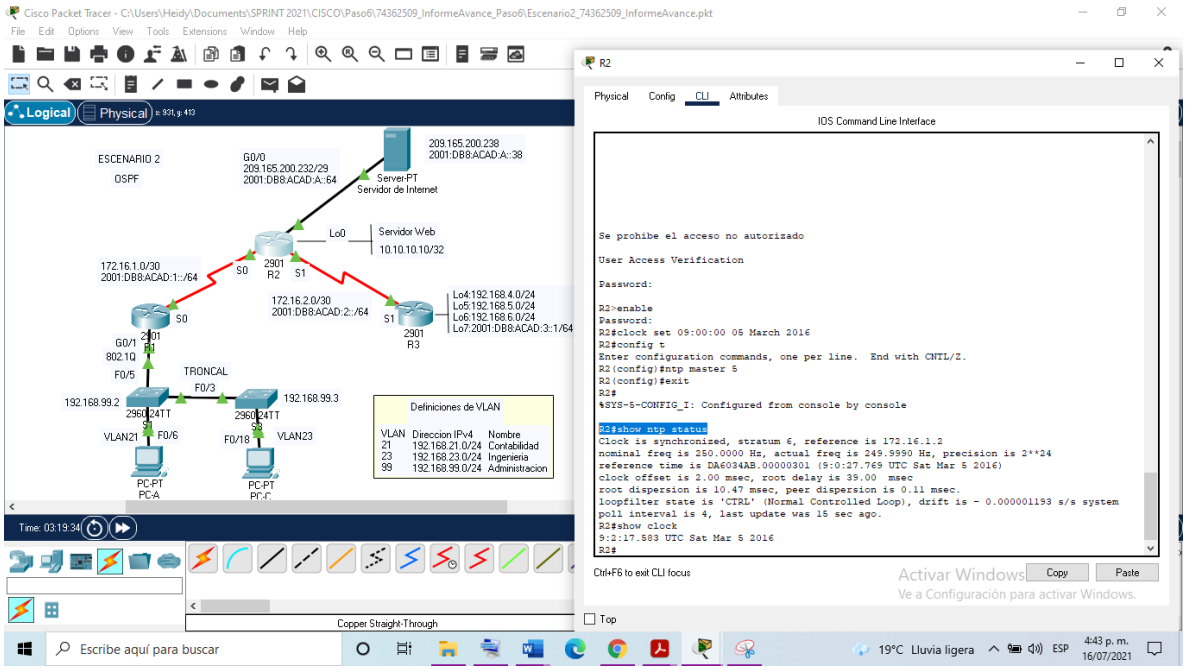

Figura 32 Verificación de la configuración NTP en R2. Fuente: propia

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

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

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

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 standart ADMIN-MGT R2(config)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#line vty 0 4 R2(config)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

Tabla 33 configuración y verificación de las listas de control de acceso ACL

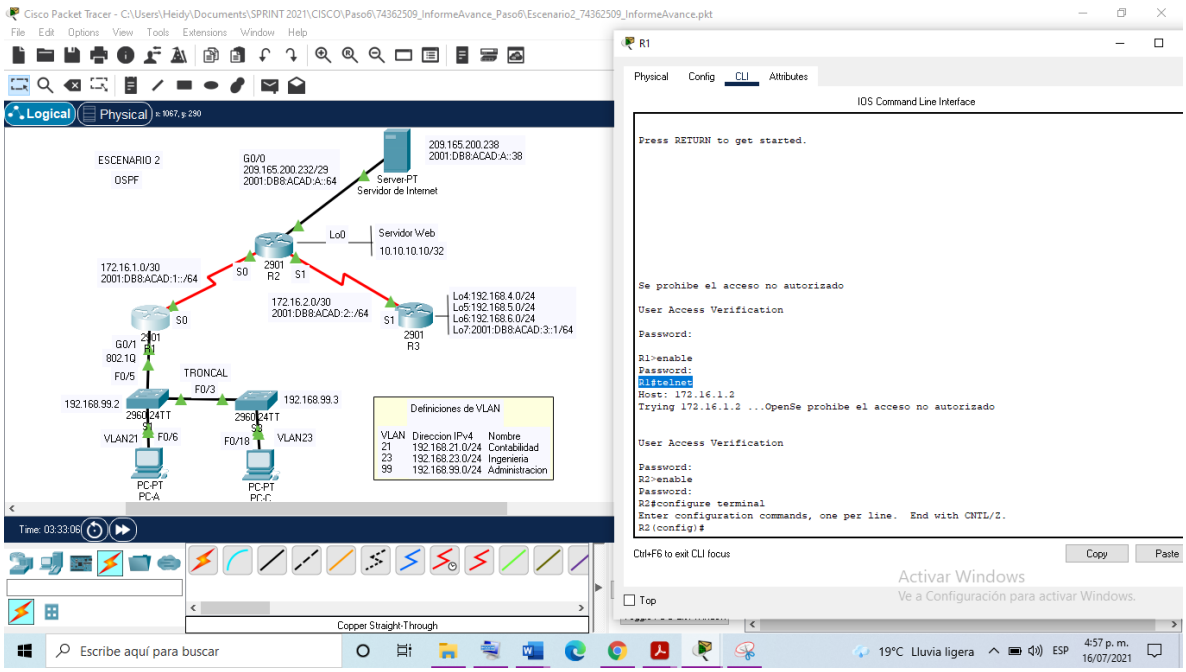

Figura 33 Verificación de que ACL funciona. Fuente: propia

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	# show access-lists
Restablecer los contadores de una lista de acceso	# clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	# show ip interface | include Access #show running-config | include access
¿Con qué comando se muestran las traducciones NAT?	#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translations

Tabla 34 Verificaciones de las configuraciones realizadas en la red

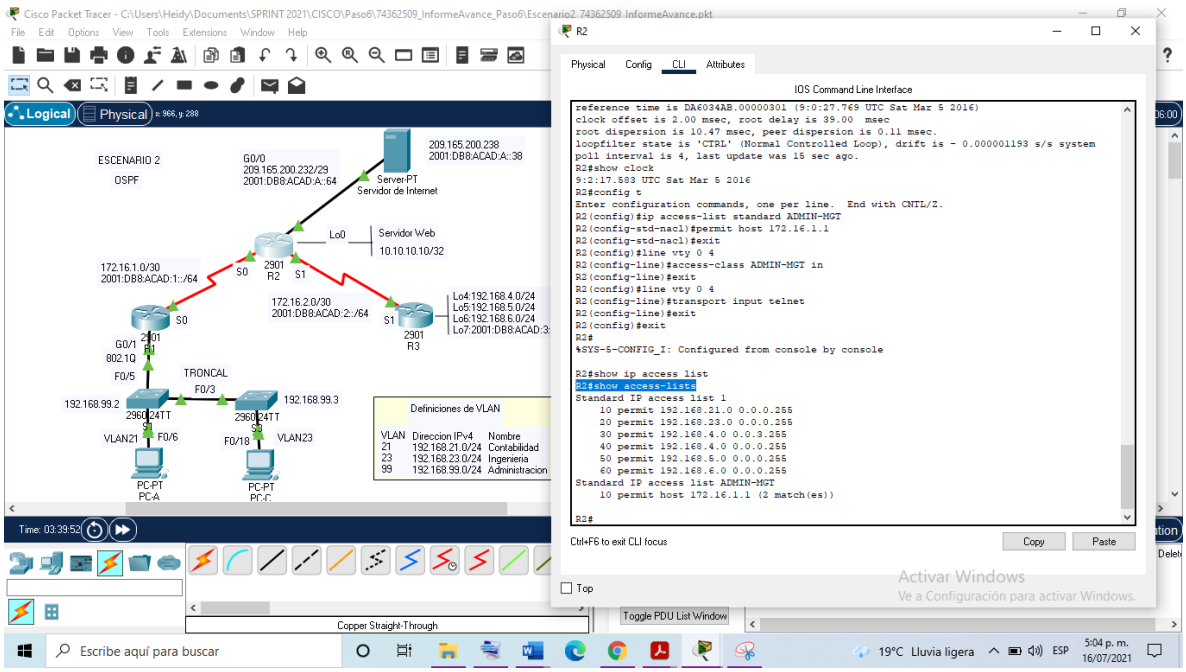

Figura 34 Verificación del comando show access-list en R2. Fuente: propia

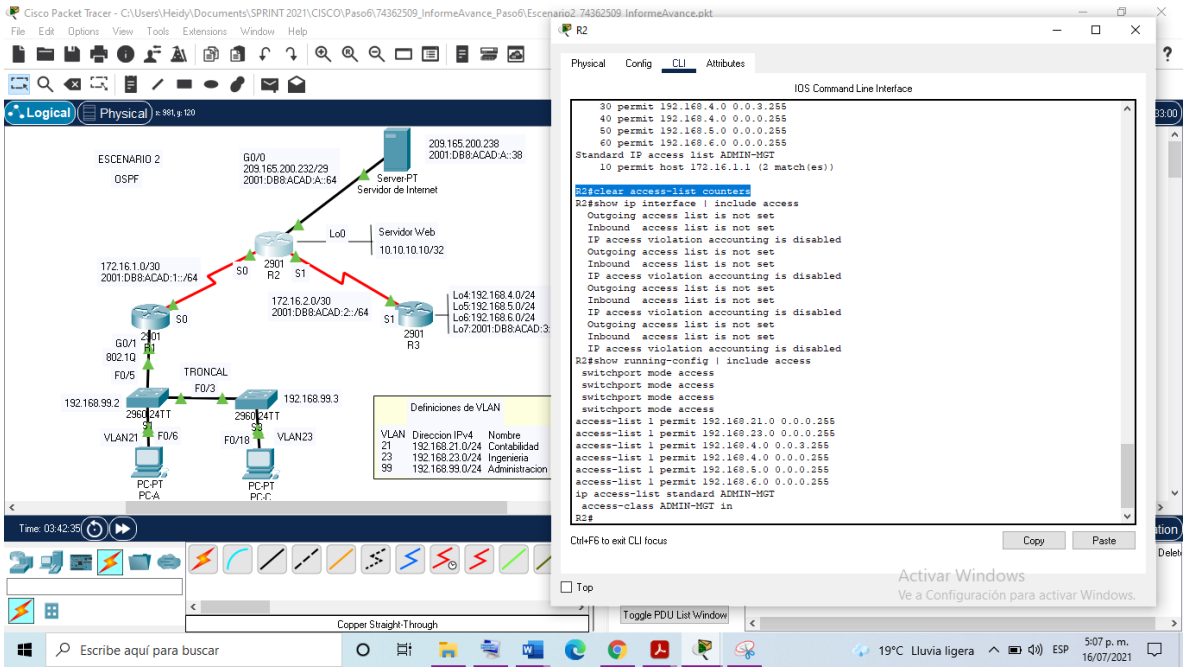

Figura 35 Verificación del comando show ip interface. Fuente: propia

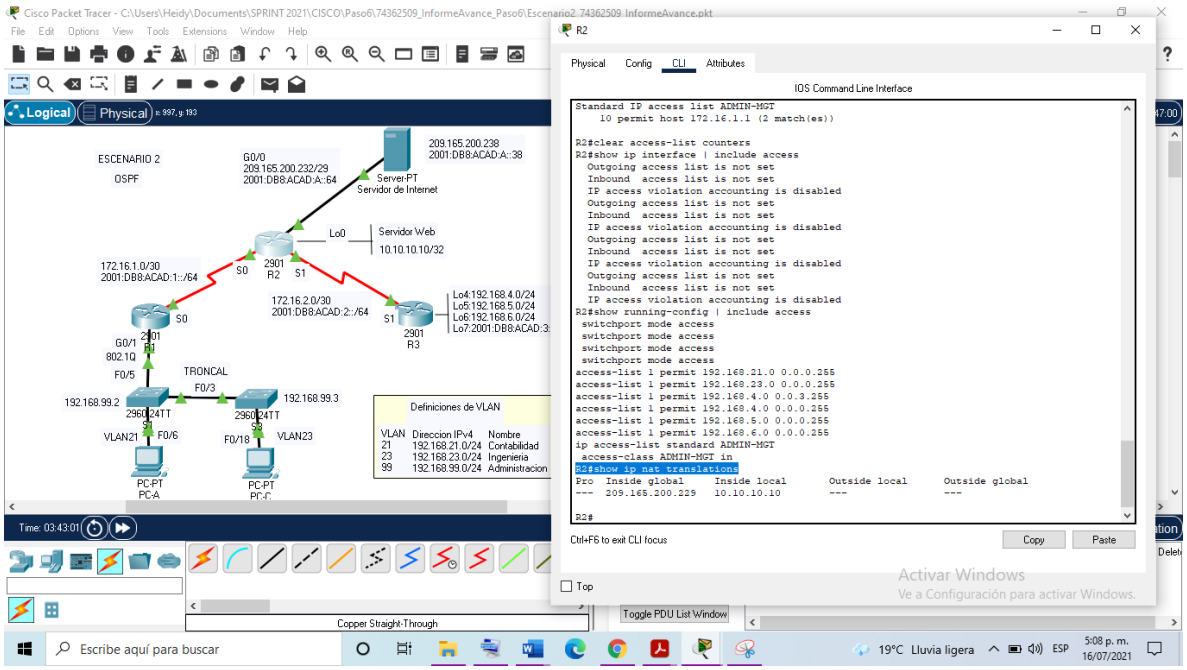

Figura 36 Verificación del comando show ip nat translations. Fuente: propia

CONCLUSIONES

El proceso de configuración de los dispositivos en un principio parece ser algo demasiado difícil pero una vez, tenemos claros el comando y gracias a los capítulos dentro de la plataforma se puede solventar muchas de las dudas que se generan al momento de encaminarse al resolver la actividad.

Aunque la plataforma cisco tiene gran variedad de dispositivos de internet working, es fundamental conocerlos y saber cómo configurar de manera correcta para poder integrarlos a una red.

El direccionamiento Ip es el número de identificación de los dispositivos conectados a una red, el direccionamiento Ipv4 es el direccionamiento que se ha usado desde la invención del internet, debido a la gran cantidad de usuarios que hoy en día se conectan a internet, y el número limitado de conexiones que posee el Ipv4 que es aprox. 4.3 mil millones de direcciones, se está evolucionando a direccionamiento Ipv6 estos pensado en las generaciones futuras ya que con ipv6 conseguimos un numero de (18,446,744,073,709,551,616) direcciones IP posibles.

Con un correcto direccionamiento en las redes es posible realizar conexión entre los equipos que la conforman, con un correcto Subneteo es posible proporcionar un mejor manejo de la red y garantizar la interconexión deseada.

Para realizar un buen direccionamiento es de suma importancia realizar correctamente la tabla de subredes para así facilitar el proceso de asignación y configuración de subredes en los equipos. Si todos los equipos pertenecen a una misma subred es posible la conexión entre los diferentes equipos que conforman la red y cuando los equipos se encuentran dentro de la misma subred los datos pueden ser enviados directamente sin necesidad de desvíos de comunicación.

REFERENCIAS

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

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

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

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

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

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

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

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

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

Syllabus del curso Diplomado de profundización CISCO CCNA (2021). Disponible en: https://campus129.unad.edu.co/ecbti90/mod/folder/view.php?id=3858