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

ALEX FERNANDO FORERO ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

SANTA MARTA

2021

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

ALEX FERNANDO FORERO ACUÑA

Diplomado de profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN)

Director /Tutor

MSc.JAVIER RICARDO VASQUEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

SANTA MARTA

2021

NOTA DE ACEPTACIÓN:

Aprobado por el comité y Director del Diplomando de Profundización CISCO. “Diseño e implementación de soluciones integradas LAN / WAN” Dando cumplimiento a los requisitos de opción de grado por la Universidad Nacional Abierta y a Distancia UNAD. CEAD Bogotá – Centro Jose´Acevedo y Gómez .

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Santa Marta, (octubre 18, 2021)

DEDICATORIA

Dedicaré este esfuerzo a mi esposa Shilena por su apoyo incondicional de lograr esta carrera de Ingeniería de sistemas, a mi familia quienes son mi apoyo que hacen parte fundamental de este proceso.

AGRADECIMIENTO

Agradecer a mi esposa por su apoyo y espacio para llevar a feliz término este proceso y han tenido la paciencia para brindarme los espacios de formación.

Agradecimiento especial a toda mi familia de la UNAD, tutores, Directivos, compañeros y a todos los que, con su paciencia, sapiencia y entrega me dieron los medios y la orientación en el desarrollo de este proceso de formación.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURA

RESUMEN

El trabajo se realiza con el propósito de ejecutar de una forma práctica, los conocimientos adquiridos a lo largo del Diplomado De Profundización CISCO (Diseño e Implementación de soluciones integradas LAN/WAN), aportando al estudiante las habilidades necesarias en el manejo de redes, enfrentándolo a dos escenarios, en donde para cada uno de ellos debe construir su topología. En el escenario 1 se desarrollan los conocimientos en cuanto a la configuración de los equipos descritos en una topología y en una tabla, la cual contiene el direccionamiento de cada uno de ellos, así como los servicios DHCP, RIPv2, enlaces troncales y la implementación de NAT. En cuanto al escenario 2, se evalúan las competencias en la implementación del enrutamiento por OSPFv2, habilitar y deshabilitar DNS, al igual que NAT y VLAN.

ABSTRACT

The work is carried out with the purpose of executing in a practical way, the knowledge acquired throughout the CISCO Deepening Diploma (Design and Implementation of integrated LAN / WAN solutions), providing the student with the necessary skills in network management, facing it to two scenarios, where for each of them you must build your topology. In scenario 1, knowledge is developed regarding the configuration of the equipment described in a topology and in a table, which contains the addressing of each one of them, as well as the DHCP, RIPv2, trunk links and the implementation of NAT. Regarding scenario 2, the competencies in the implementation of routing by OSPFv2, enable and disable DNS, as well as NAT and VLAN are evaluated.

GLOSARIO

Banda: Conjunto de las frecuencias comprendidas entre límites determinados y pertenecientes a un espectro o gama de mayor extensión. La clasificación adoptada internacionalmente está basada en bandas numeradas que van de la que se ubica de los 0.3 x 10n Hz a 3 x 10n Hz, en la cual n es el número de banda.

Dirección IP: Una dirección en la red asignada a una in-terfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Dirección IPv6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2128 vs. 232). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

ICPM (Internet Control Message Protocol, Protocolo de mensajes de control de Internet): Es un protocolo que permite administrar información relacionada con errores de los equipos en red

ISP (Internet Services Provider/Proveedor de Servicios de Internet): Una compañía que proporciona a sus clientes acceso a Internet.

Kernel (del Inglés Núcleo): En informática, el núcleo (también conocido en español con el anglicismo kernel, de raíces germánicas como kern) es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware del computador o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema. Como hay muchos programas y el acceso al hardware es limitado, el núcleo

también se encarga de decidir qué programa puede hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado

INTRODUCCIÓN

En el presente informe se demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este. Se configurarán los dispositivos en cada uno de los escenarios y al final se verificarán si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

El simulador aplicado para el desarrollo de los dos escenarios es la aplicación propietaria de CISCO denominado Packet Tracer que permite las configuraciones básicas de switches y routers. Además, la configuración de interoperabilidad de protocolos IPv4 e IPv6, protocolos de enrutamiento, seguridad, aplicación de redes virtuales VLAN, direccionamiento dinámico, establecimiento de listas de control de acceso y traducción de direcciones de red NAT.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Rendir un informe de los requerimientos adelantados durante el Diplomando de Profundización CISCO aplicando las competencias y habilidades desarrolladas durante el proceso académico dando respuesta y solución a cada uno de los escenarios planteados.

2.2 OBJETIVOS ESPECÍFICOS

Conceptualizar las temáticas planteadas en los dos escenarios del Diplomado de profundización CCNA.

Implementar las topologías propuestas en un entorno de simulación evaluando los requerimientos y alternativas de solución.

Configurar los dispositivos: router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6, protocolos de enrutamiento, creación de VLAN's, NAT, listas de control de acceso y seguridad con los comandos diseñados para tal fin.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1
Topología

figura 1. Topología escenario 1

Figura 1: Topología Escenario 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

figura 2. Construcción de la red

propia autoria.

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Se realiza la implementación de la topología

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. direccionamiento

<table>
<tr><th>Item</th><th>Requerimiento</th></tr>
<tr><td>Dirección de Red</td><td>192.168.39.0 donde 39 corresponde a los últimos dos dígitos de su cédula.</td></tr>
<tr><td>Requerimiento de host Subred LAN1</td><td>100
<table>
<tr><th>direcion de red</th><th>primera ip asignable</th><th>ultima ip asignable</th><th>direccion de broadcast</th></tr>
<tr><td>192.168.39.0/25</td><td>192.168.39.1/25</td><td>192.168.39.126/25</td><td>192.168.39.127/25</td></tr>
</table>
Mascara de subred
255.255.255.128</td></tr>
<tr><td>Requerimiento de host Subred LAN2</td><td>50
<table>
<tr><th>direcion de red</th><th>primera ip asignable</th><th>ultima ip asignable</th><th>direccion de broadcast</th></tr>
<tr><td>192.168.39.128/26</td><td>192.168.39.129/26</td><td>192.168.39.190/26</td><td>192.168.39.191/26</td></tr>
<tr><td>192.168.39.192/26</td><td>192.168.39.253/26</td><td>192.168.39.254/26</td><td>192.168.39.255/26</td></tr>
</table>
Mascara de subred</td></tr>
</table>

	255.255.255.192
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.39.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.39.129/26
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.39.2/25
PC-A	Última dirección de host de la subred LAN1 192.168.39.126/25
PC-B	Última dirección de host de la subred LAN2 192.168.39.190/26

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración de los ajustes básicos R1.

Tarea	Especificación
Desactivar la búsqueda DNS	Router> Router>**enable**

	Router# **configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router	Router(config)#**hostname R1** R1(config)#
Nombre de dominio	R1(config)#**ip domain-name ccna-lab.com** R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#**enable secret ciscoenpass** R1(config)#
Contraseña de acceso a la consola	R1(config)#**line console 0** R1(config-line)#**password ciscoconpass** R1(config-line)#**login** R1(config-line)#**exit** R1(config)#
Establecer la longitud mínima para las contraseñas	R1(config)#**security passwords min-length 10** R1(config)#
Crear un usuario administrativo en la base de datos local	R1(config)#**username admin password admin1pass** R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#**line vty 0 15** R1(config-line)#**login local** R1(config-line)#**exit** R1(config)#

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** R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#
Configure un MOTD Banner	R1(config)#**banner motd # *** CCNA - Acceso restringido *** #** R1(config)#
Configurar interfaz G0/0/0	R1(config)#**interface gigabitEthernet 0/0/0** R1(config-subif)#**encapsulation dot1Q 2** R1(config-subif)#**description Vlan2 Bikes** R1(config-subif)#**ip address** 192.168.39.129 **255.255.255.192** R1(config-if)#**no shutdown** R1(config-if)#**exit** R1(config)#
Configurar interfaz G0/0/1	R1(config)#**interface gigabitEthernet 0/0/1** R1(config-subif)#**encapsulation dot1Q 2** R1(config-subif)#**description Vlan2 Bikes** R1(config-subif)#**ip address** 192.168.39.1 **255.255.255.128** R1(config-if)#**no shutdown** R1(config-if)#**exit** R1(config)#
Generar una clave de cifrado RSA	R1(config)# R1(config)#**crypto key generate rsa 1024** R1(config)#**do wr** R1(config)#**exit**

	R1#

Se implemento en simudador packet tracer

Router>enable
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin password admin1pass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#transpor input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "CCNA-Acceso restringido"
R1(config)#int g0/0/0
R1(config-if)#description Vlan2 Bikes
R1(config-if)#ip address 192.168.39.129 255.255.255.192
R1(config-if)#no shutdown

R1(config-if)#exit
R1(config)#int g0/0/1
R1(config-if)#description Vlan2 Bikes
R1(config-if)#ip address 192.168.39.1 255.255.255.128
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

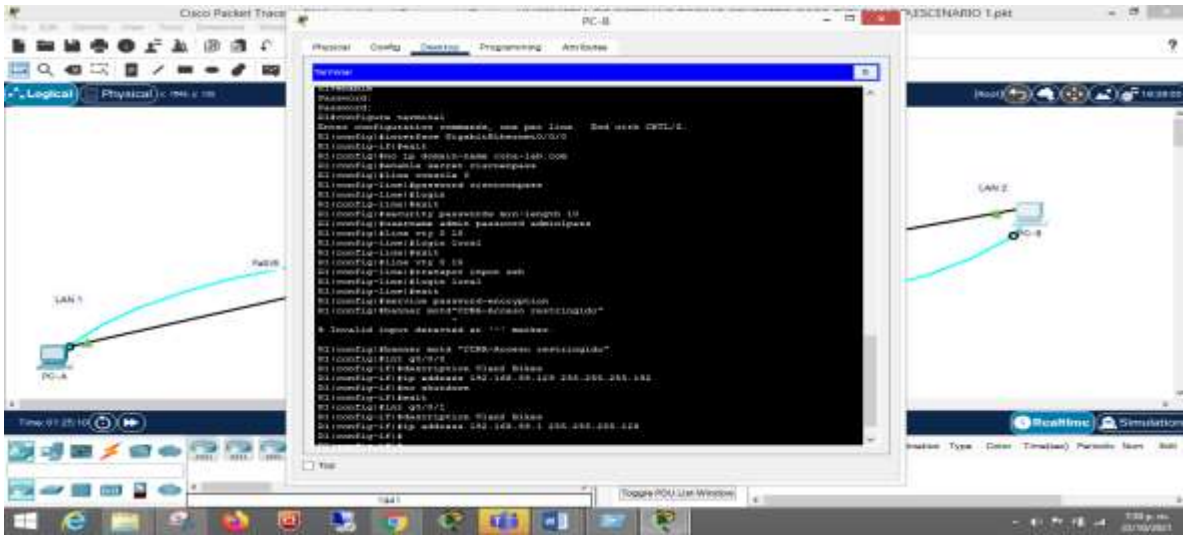
R1(config-if)#exit
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#do wr
**Mar 1 0:4:8.188: %SSH-5-ENABLED: SSH 1.99 has been enabled*
Building configuration...
[OK]
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#

figura 3 configuración R1 por medio de consola



propia autoria

Las tareas de configuración de S1 incluyen lo siguiente:

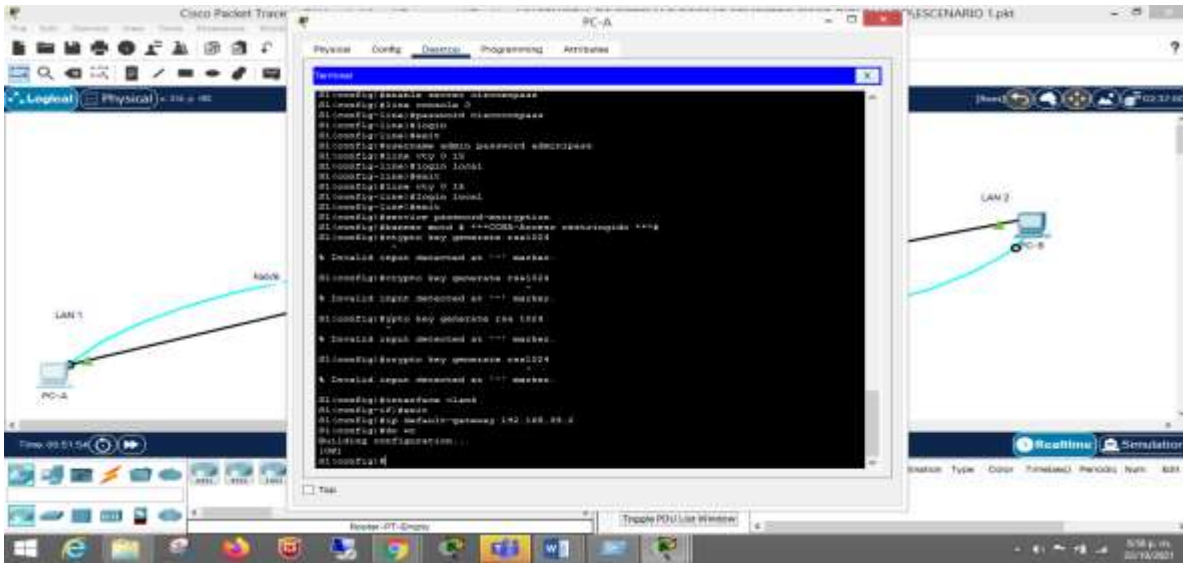
Tabla 1. Configuración de los ajustes básicos S1.

Tarea	Especificación
Desactivar la búsqueda DNS.	**Switch>** **Switch>enable** **Switch#configure terminal** **Switch(config)#no ip domain lookup**

	Switch(config)#
Nombre del switch	Switch(config)#**hostname S1** S1(config)#
Nombre de dominio	S1(config)#**ip domain-name ccna-lab.com** S1(config)#
Contraseña cifrada para el modo EXEC privilegiado	**S1(config)#enable secret ciscoenpass** **S1(config)#**
Contraseña de acceso a la consola	S1(config)#**line console 0** S1(config-line)#**password ciscoconpass** S1(config-line)#**login** S1(config-line)#**exit** S1(config)#
Crear un usuario administrativo en la base de datos local	S1(config)#**username admin password admin1pass** S1(config)#
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** **S1(config)#**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**S1(config)#line vty 0 15** **S1(config-line)#login local** **S1(config-line)#exit** **S1(config)#**

Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption** S1(config)#
Configurar un MOTD Banner	**S1(config)#banner motd # *** CCNA -** **Acceso restringido *** #** **S1(config)#**
Generar una clave de cifrado RSA	S1(config)#**crypto key generate rsa 1024** S1(config)#
Configurar la interfaz de administración (SVI)	S1(config)# S1(config)#**interface Vlan4**
Configuración del gateway predetermignado	S1(config)# S1(config)#**ip default-gateway** 192.168.39.2 S1(config)#**do wr** Building configuration... [OK] S1(config)#

figura 4 configuración S1



propia autoria

Paso 2. Configurar los equipos

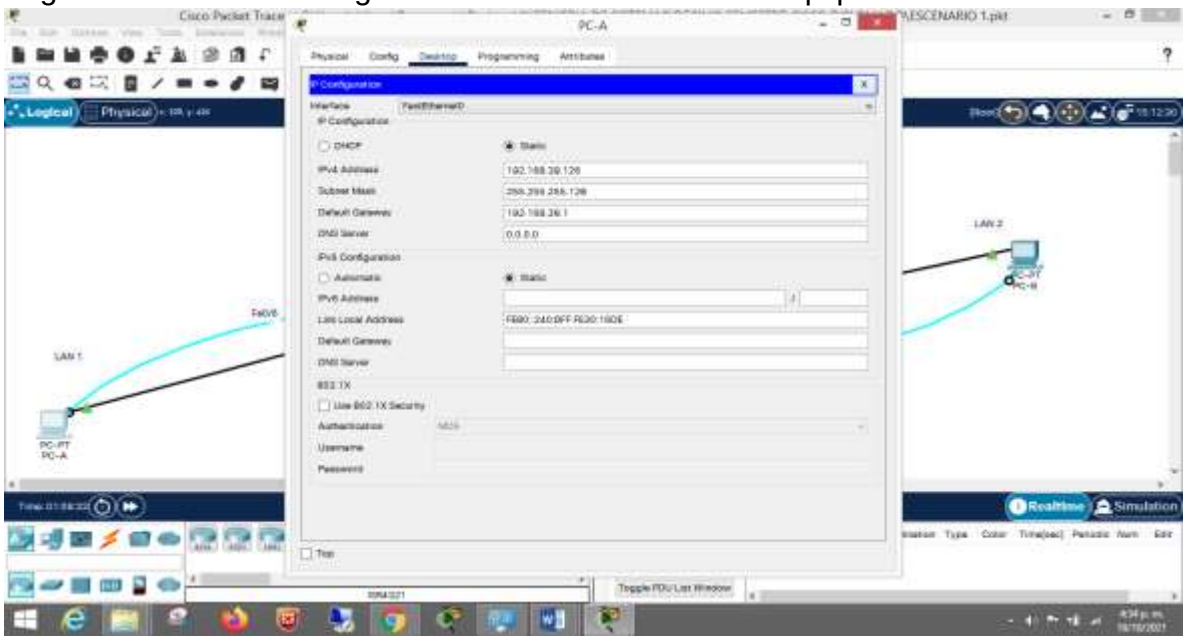
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 3. Configuración de los equipos host PC-A.

PC-A Network Configuration	
Descripción	**PC-A**
Dirección física	192.168.39.0
Dirección IP	192.168.39.126
Máscara de subred	255.255.255.128

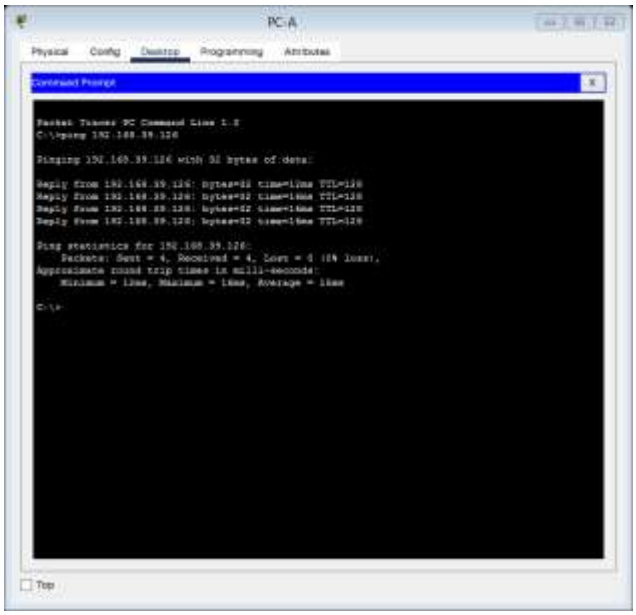
Gateway predeterminado	192.168.39.1

Figura 5. Configuración de los equipos host PC-A.



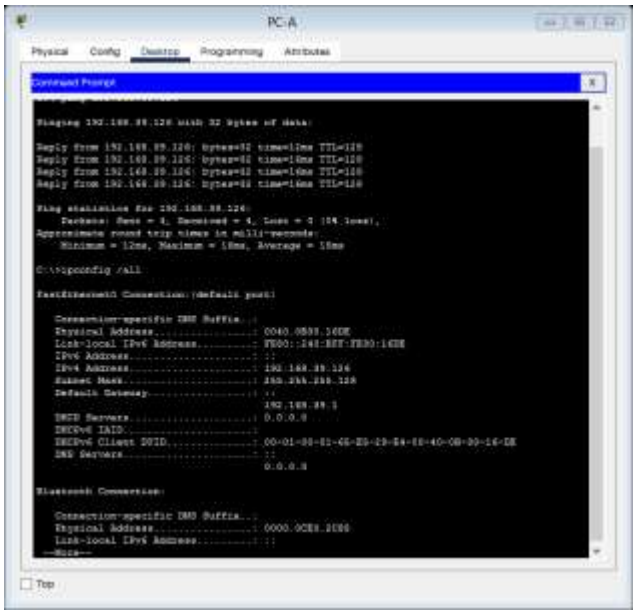
4 propia autoria

Figura 6 conectividad PC-A a 192.168.39.126



propia autoria

Figura 7 conectividad pc-A

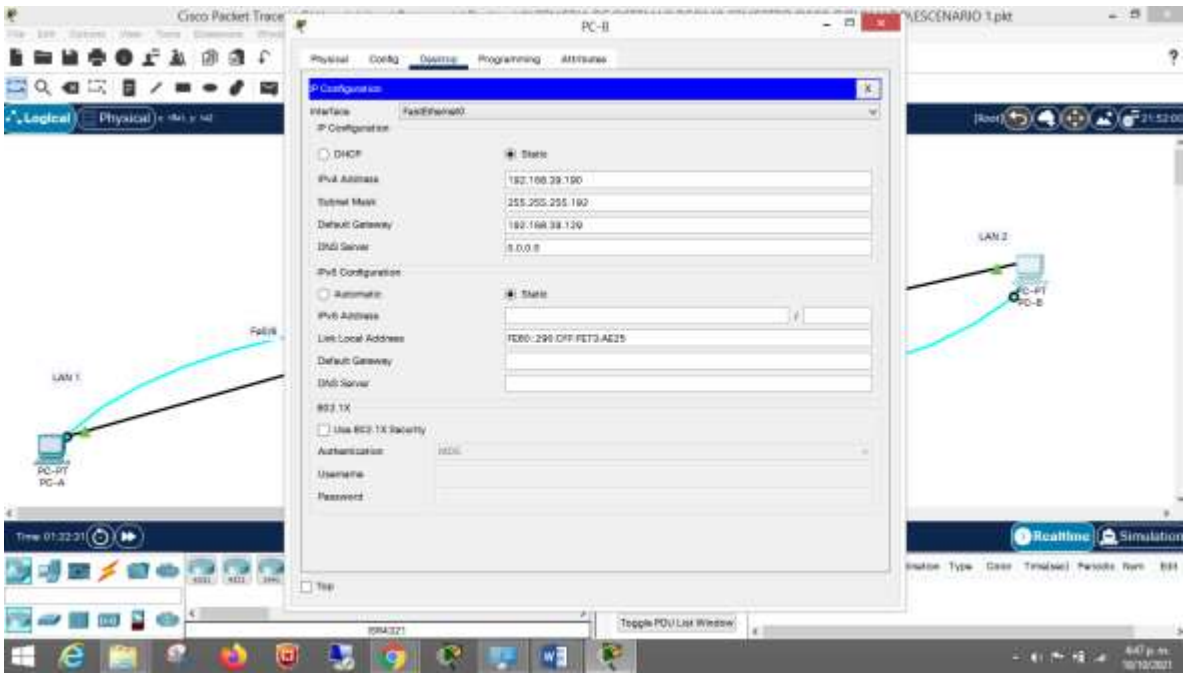


propia autoria

Tabla 4. Configuración de los equipos host PC-B.

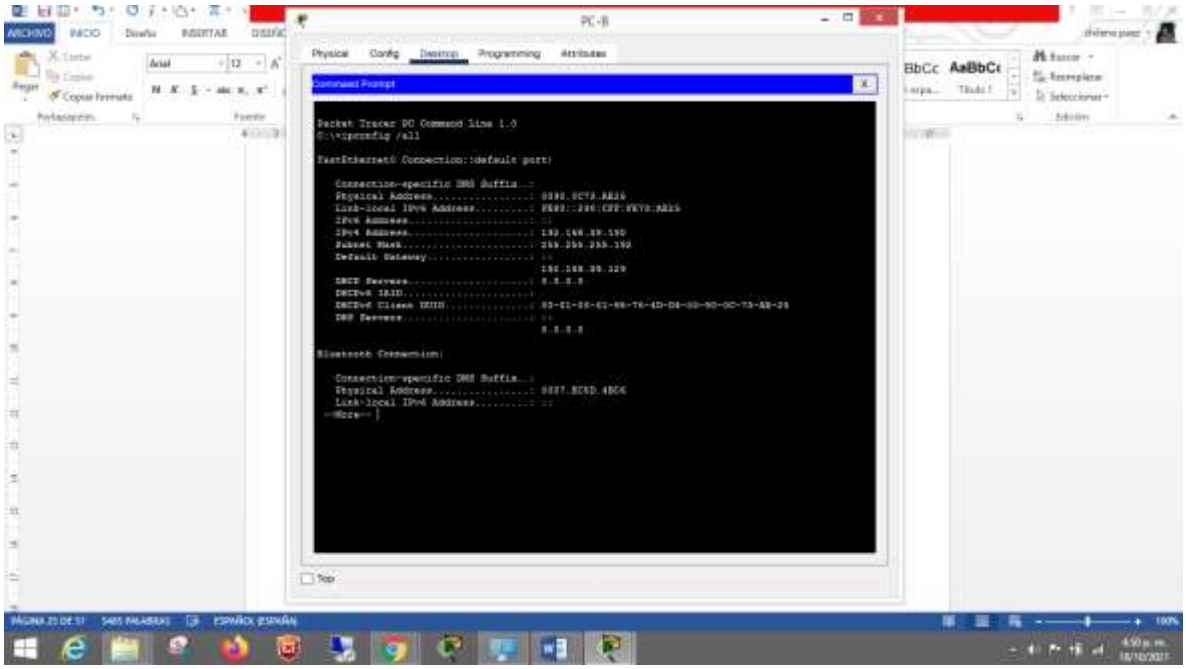
	PC-B Network Configuration
Descripción	**PC-B**
Dirección física	192.168.39.128
Dirección IP	192.168.39.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.39.129

Figura 8 configuracion de PC-B



propia autoria

Figura 9 conectividad PC-B IPCONFIG/ALL

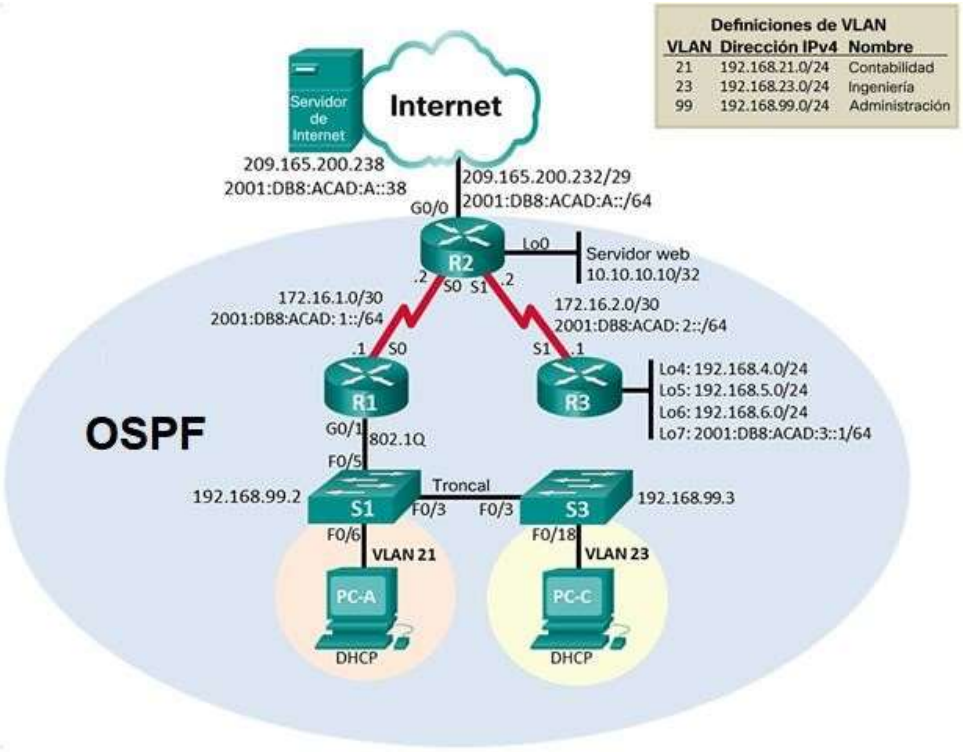


propia autoria

Escenario 2

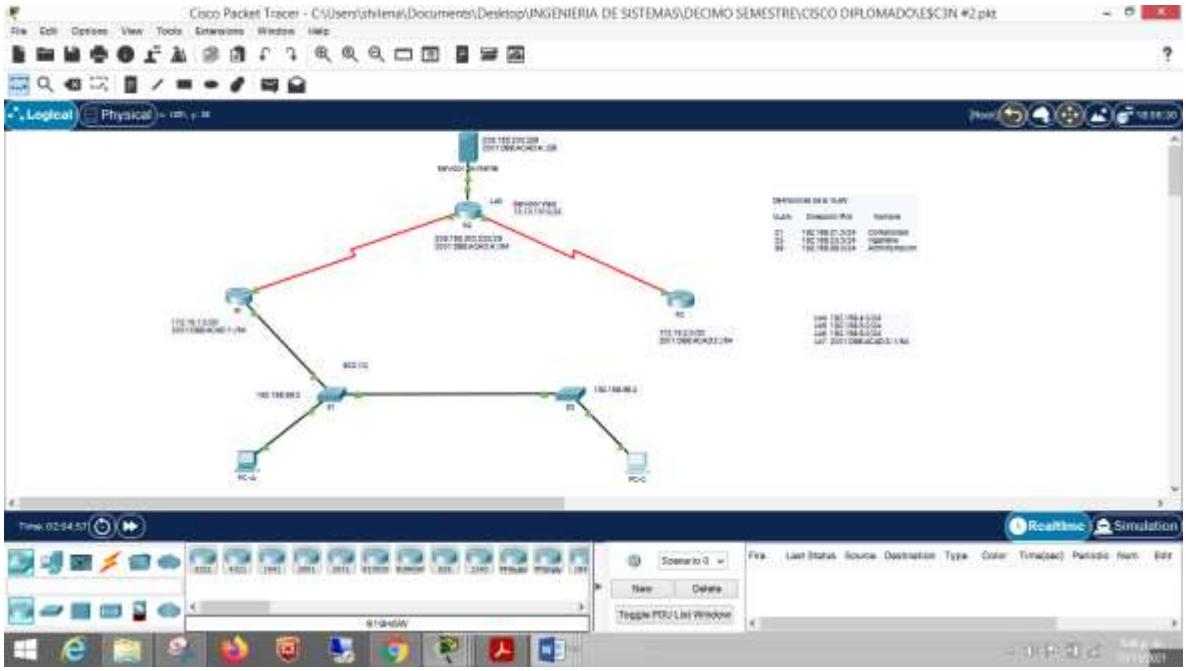
Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de 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.

Topología



Parte 1: Inicializar dispositivos

Figura 10.Construcción de la red escenario 2



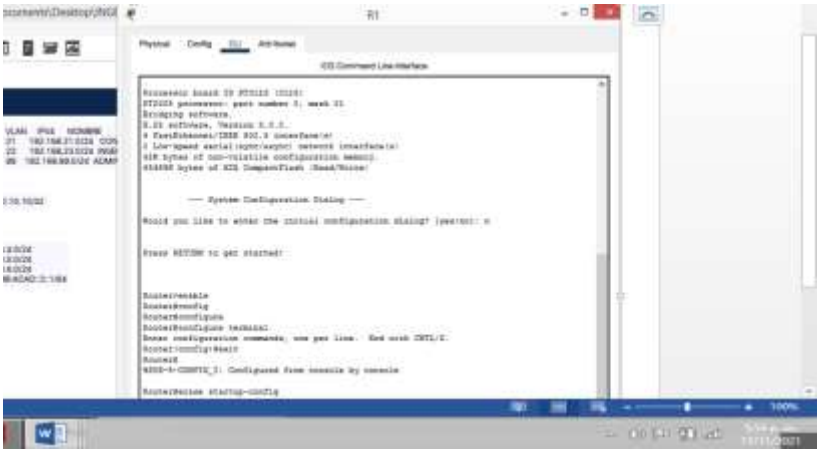
Propia autoria

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

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

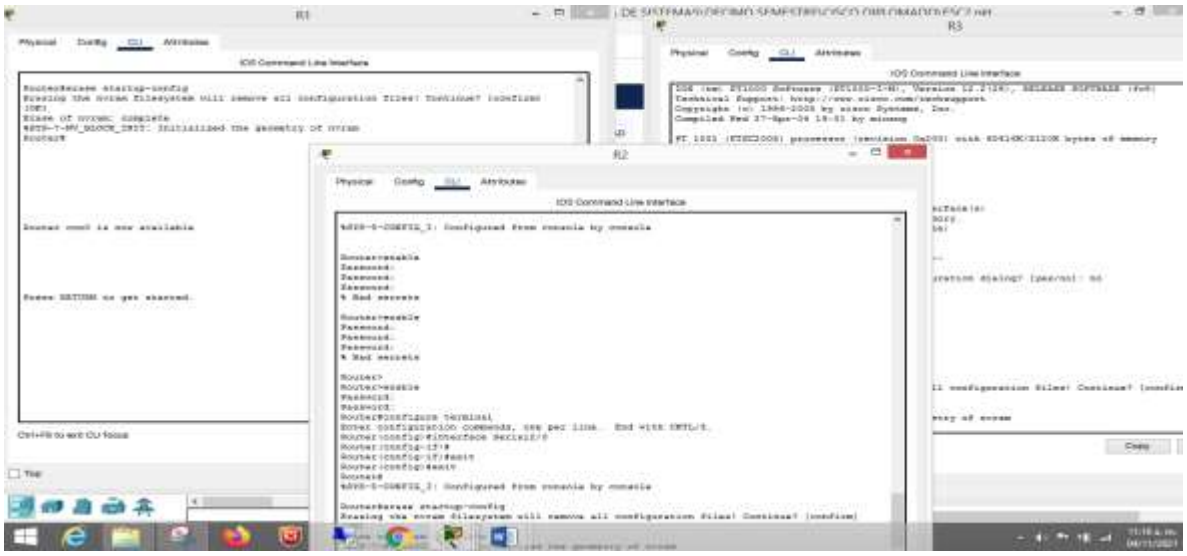
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Figura 11. Iniciando Router y switches



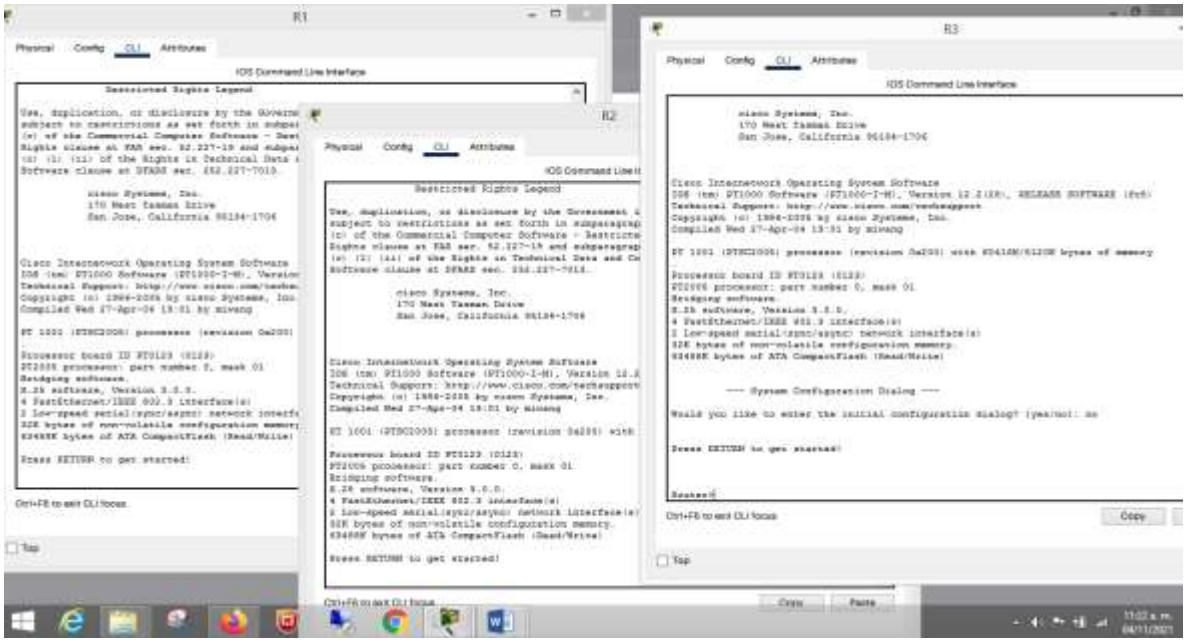
Propia autoria

Figura 12.configuracion de R1,R2,R3



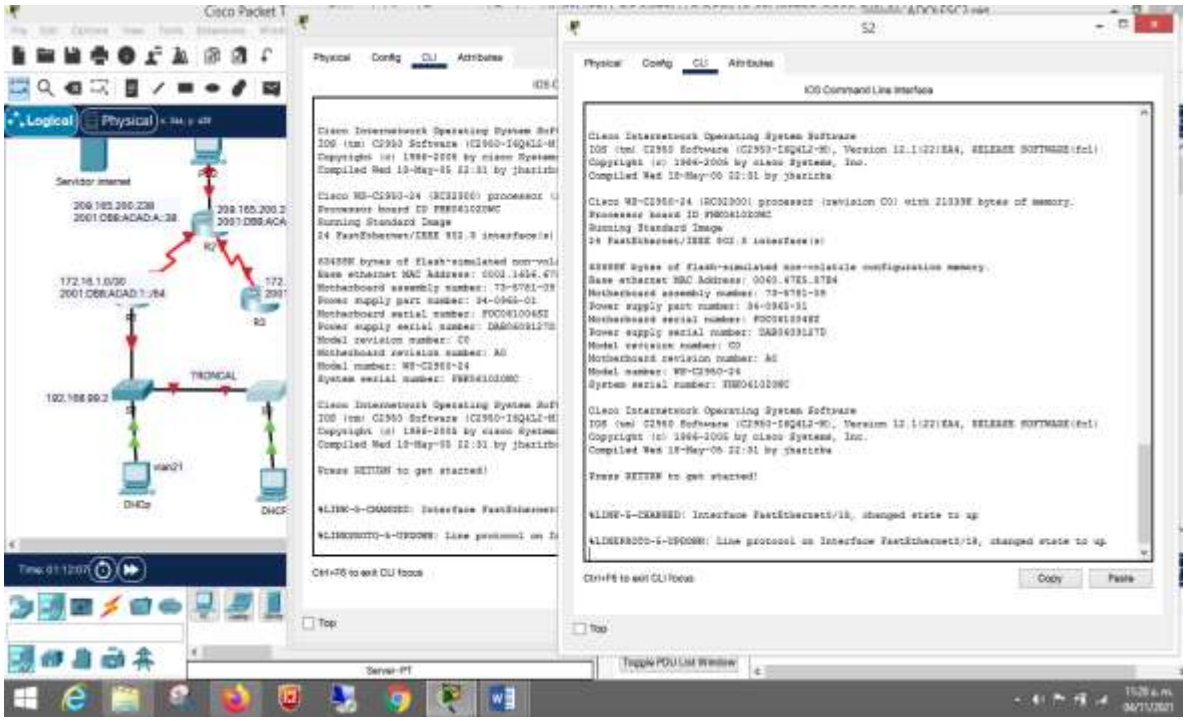
Propia autoria

Figura 13. Configuración Router



Propia autoria

Figura 14. Configuración de switches



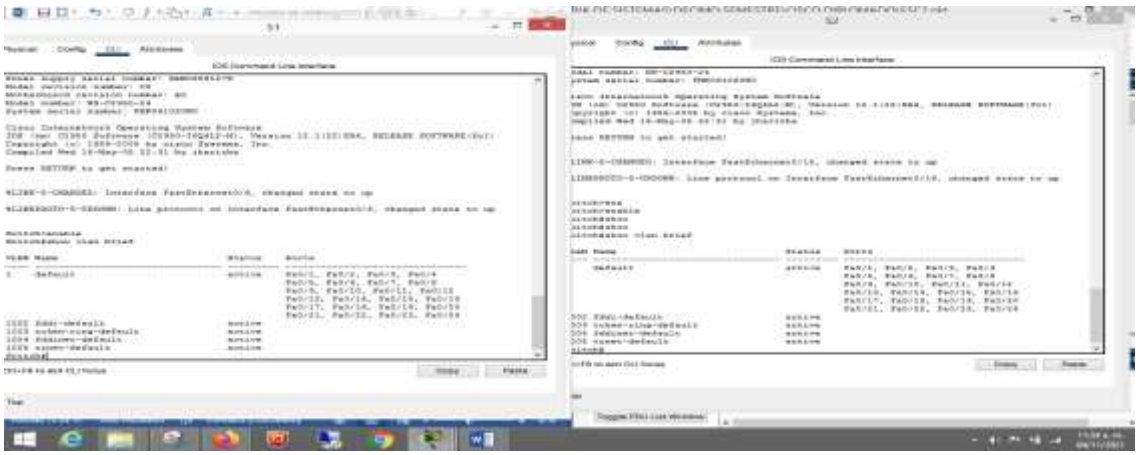
Propia autoria

Tabla N. 5 Inicialización y carga de routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Configuración Routers **R1, R2 y R3** Router> Router>**enable** Router# **erase startup-config** Continue? [confirm] [**Enter**] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Configuración Routers **R1, R2 y R3** Router# **reload** Proceed with reload? [confirm] [**Enter**] Router>

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Configuración Switches **S1 y S2** Switch# Switch#**erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [Enter] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Configuración Switches **S1 y S2** Switch# Switch# **reload** Proceed with reload? [confirm] [**Enter**] Switch>
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# Switch#**show vlan brief** Switch#

Figura 15. Inicialización y carga de switches



Propia autoria

Parte 2: Configurar los parámetros básicos de los dispositivos

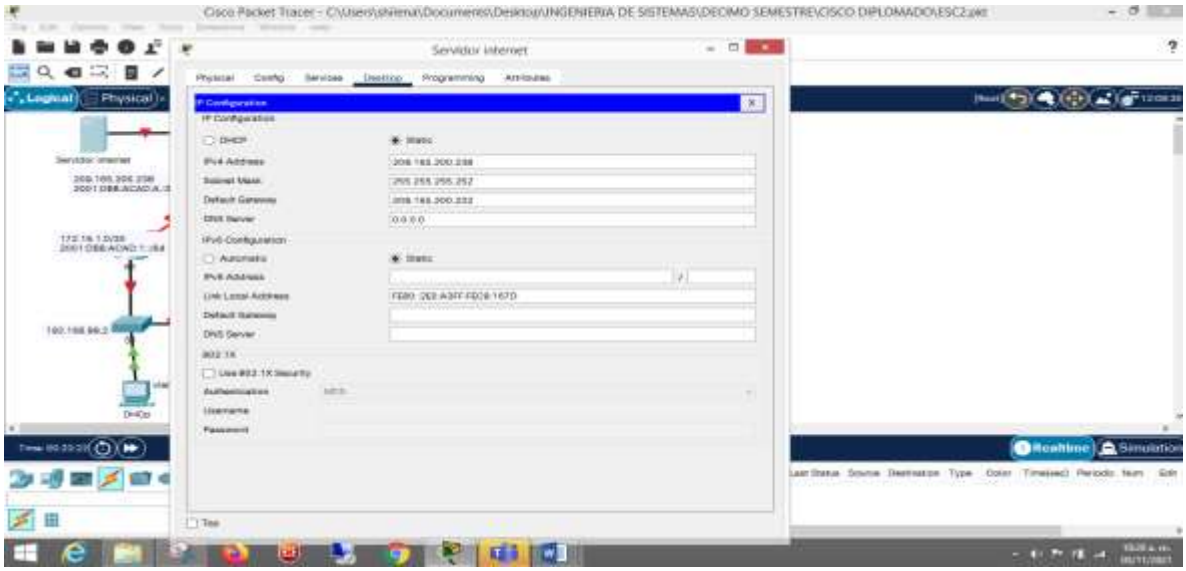
Paso 1: Configurar la computadora de Internet

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

Tabla N. 6 Configuraracion de la computadora de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.252
Gateway predeterminado	209.165.200.232/29
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:A::/64

Figura 16.configurado servidor inernet



Propia autoria

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Tabla N. 7 Configuracion R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router	Router>**enable** Router# **configure terminal** Router(config)#**hostname R1**
Contraseña de exec privilegiado cifrada	R1>enable R1# **configure terminal** R1(config)# **enable secret class** R1(config)#**exit**
Contraseña de acceso a la consola	R1>enable R1# **configure terminal** R1(config)# **line console 0** R1(config-line)# **password cisco** R1(config-line)# **login** R1(config-line)# **exit** R1(config)#**exit**
Contraseña de acceso Telnet	R1#**configure terminal** R1(config)#**line vty 0 4** R1(config-line)#**password cisco** R1(config-line)# **login** R1(config-line)#**exit** R1(config)#
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#**exit**
Mensaje MOTD	R1#**configure terminal** R1(config)# **banner motd # *** Se prohíbe el acceso no autorizado *** #** R1(config)# **exit** R1(config)#

Interfaz S0/0/0	R1#conf ter R1(config)#**interface serial 0/0/0** **R1(config)# description connection to R2** R1(config)#**ip address 172.16.1.1 255.255.255.252** R1(config)#**ipv6 address 2001:DB8:ACAD:1::1/64** R1(config)#**clock rate 128000** R1(config)#**no shutdown** R1(config)#**exit**
Rutas predeterminadas	R1#conf ter 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)#**exit**

Nota: Todavía no configure G0/1.

Se realizo la configuración en R1

Router>enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd # Se prohbe el acceso no autorizado#
R1(config)#int s0/0/0
R1(config-if)#description connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit

R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla N. 8 Configuracion R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>**enable** Router#**configure terminal** Router(config)#**no ip domain-lookup** Router(config)#
Nombre del router	Router>**enable** Router# **configure terminal** Router(config)#**hostname R2** R2(config)#**exit**
Contraseña de exec privilegiado cifrada	R2>enable R2# **configure terminal** R2(config)# **enable secret class** R2(config)#**exit**
Contraseña de acceso a la consola	R2>enable R2# **configure terminal** R2(config)# **line console 0** R2(config-line)# **password cisco** R2(config-line)# **login** R2(config-line)# **exit** R2(config)#
Contraseña de acceso Telnet	R2#**configure terminal** R2(config)#**line vty 0 4** R2(config-line)#**password cisco** R2(config-line)# **login** R2(config-line)#**exit** R2(config)#

Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption** R1(config)#**exit**
Habilitar el servidor HTTP	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http server** R2(config)#**exit** R2#
Mensaje MOTD	R2# **configure terminal** R2(config)# **banner motd # *** Se prohibe el acceso no autorizado *** #** R2(config)# exit
Interfaz S0/0/0	R2#config t R2(config)# **interface serial 0/0/0** R2(config)# **description connection to R1** R2(config)# **ip address 172.16.1.2 255.255.255.252** R2(config)# **ipv6 address 2001:DB8:ACAD:1::2/64** R2(config)# **no shutdown** R2(config)# **exit** R2#
Interfaz S0/0/1	R2#config t R2(config)# **interface serial 0/0/1** R2(config)# **description Conexion a R3** R2(config)# **ip address 172.16.2.2 255.255.255.252** R2(config)# **ipv6 address 2001:DB8:ACAD:2::2/64** R2(config)# **clock rate 128000** R2(config)# **no shutdown** R2(config)# **exit** R2#
Interfaz G0/0 (simulación de Internet)	R2#config t R2(config)# **interface gigabitEthernet 0/0** R2(config)# **description connection to Internet** R2(config)# **ip address 209.165.200.233 255.255.255.248** R2(config)# **ipv6 address 2001:DB8:ACAD:A::1/64**

	R2(config)# **no shutdown** R2(config)# **exit** R2#
Interfaz loopback 0 (servidor web simulado)	R2#config t R2(config)# **interface loopback 0** R2(config)# **description Simulated Web Server** R2(config)# **ip address 10.10.10.10 255.255.255.255** R2(config)# **exit** R2#
Ruta predeterminada	R2#config ter R2(config)# **ip route 0.0.0.0 0.0.0.0 g0/0** R2(config)# **ipv6 route ::/0 g0/0** R2(config)# **exit** R2#

Router>enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#banner motd # Se prohibe el acceso no autorizado #
R2(config)#int s0/0/0
R2(config-if)#description connection to R1
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
R2(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R2(config)#int s0/0/1
R2(config-if)#description connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#int g0/0
R2(config-if)#description connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:db8:acad:a::1/64
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#int loopback 0
R2(config-if)#description Simulated Web Server
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla N.9 configuracion R3

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

	R3#
Interfaz S0/0/1	R3#config t R3(config)# **interface serial 0/0/1** R3(config)# **description connection to R2** R3(config)# **ip address 172.16.2.1 255.255.255.252** R3(config)# **ipv6 address 2001:DB8:ACAD:2::1/64** R3(config)# **no shutdown** R3(config)# **exit** R3#
Interfaz loopback 4	R3#config t R3(config)#**interface loopback 4** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 4)** R3(config)# **ip address 192.168.4.1 255.255.255.0** R3(config)# **exit** R3#
Interfaz loopback 5	R3#config t R3(config)# **interface loopback 5** R3(config)# **description Interfaz virtual (para pruebas, en este caso el 5)** R3(config)# **ip address 192.168.5.1 255.255.255.0** R3(config)#**exit** R3#
Interfaz loopback 6	R3#config t R3(config)#**interface loopback 6** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 6)** R3(config)#**ip address 192.168.6.1 255.255.255.0** R3(config)#**exit** R3#
Interfaz loopback 7	R3#config t R3(config)#**interface loopback 7** R3(config)#**description Interfaz virtual (para pruebas, en este caso el 7)** R3(config)#**ip address 2001:DB8:ACAD::3::1/64** R3(config)#**exit**

	R3#
Rutas predeterminadas	R3#config t R3(config)#**ip route 0.0.0.0 0.0.0.0 s0/0/1** R3(config)#**ipv6 route ::/0 s0/0/1** R3(config)#**exit** R3#

Router>enable
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd # Se prohibe el acceso no autorizado#
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:db8:acad:2::1/64
R3(config-if)#no shutdown
R3(config-if)#

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:
Tabla N.10 configuracion S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain-lookup** Switch(config)#**exit** Switch#
Nombre del switch	switch# **configure terminal** switch(config)#**hostname S1** S1(config)#**exit** S1#
Contraseña de exec privilegiado cifrada	S1#**configure terminal** S1(config)# **enable secret class** S1(config)#**exit** S1#
Contraseña de acceso a la consola	S1#**configure terminal** S1(config)# **line console 0** S1(config-line)# **password cisco** S1(config-line)# **login** S1(config-line)# **exit** S1(config)#**exit** S1#
Contraseña de acceso Telnet	S1#**configure terminal** S1(config)#**line vty 0 4** S1(config-line)#**password cisco** S1(config-line)# **login** S1(config-line)#**exit** S1(config)#**exit** S1#
Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption** S1(config)#**exit** S1#
Mensaje MOTD	S1#**configure terminal**

	S1(config)#**banner motd # *** Se prohibe el acceso no autorizado *** #** S1(config)#**exit** S1#

Switch>enable
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd # Se prohibe el acceso no autorizado #
S1(config)#exit
S1#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:
Tabla N. 11 Configuracion S3

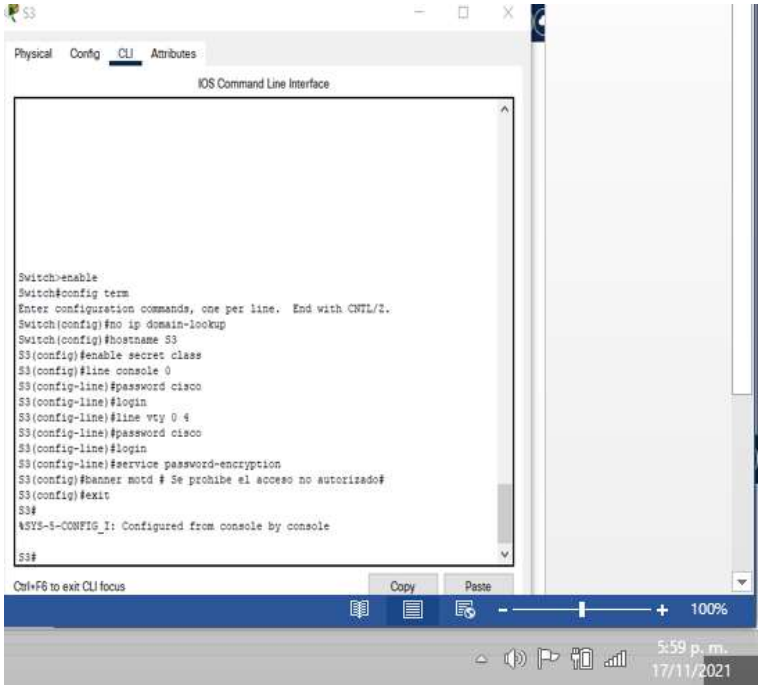
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>**enable** Switch#**configure terminal** Switch(config)#**no ip domain-lookup** Switch(config)#**exit** Switch#
Nombre del switch	switch# **configure terminal** switch(config)#**hostname S3** S3(config)#**exit** S3#

Contraseña de exec privilegiado cifrada	S3# **configure terminal** S3(config)# **enable secret class** S3(config)#**exit** S3#
Contraseña de acceso a la consola	S3#**configure terminal** S3(config)# **line console 0** S3(config-line)# **password cisco** S3(config-line)# **login** S3(config-line)# **exit** S3(config)#**exit** S3#
Contraseña de acceso Telnet	S3#**configure terminal** S3(config)#**line vty 0 4** S3(config-line)#**password cisco** S3(config-line)# **login** S3(config-line)#**exit** S3(config)#**exit** S3#
Cifrar las contraseñas de texto no cifrado	S3(config)#**service password-encryption** S3(config)#**exit** S3#
Mensaje MOTD	S3#**configure terminal** S3(config)#**banner motd # *** Se prohibe el acceso no autorizado *** #** S3(config)#**exit** S3#

Switch>enable
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login

S3(config-line)#service password-encryption
S3(config)#banner motd # Se prohibe el acceso no autorizado#
S3(config)#exit
S3#

Figura 17. Configuración S3



Autoria propia

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:

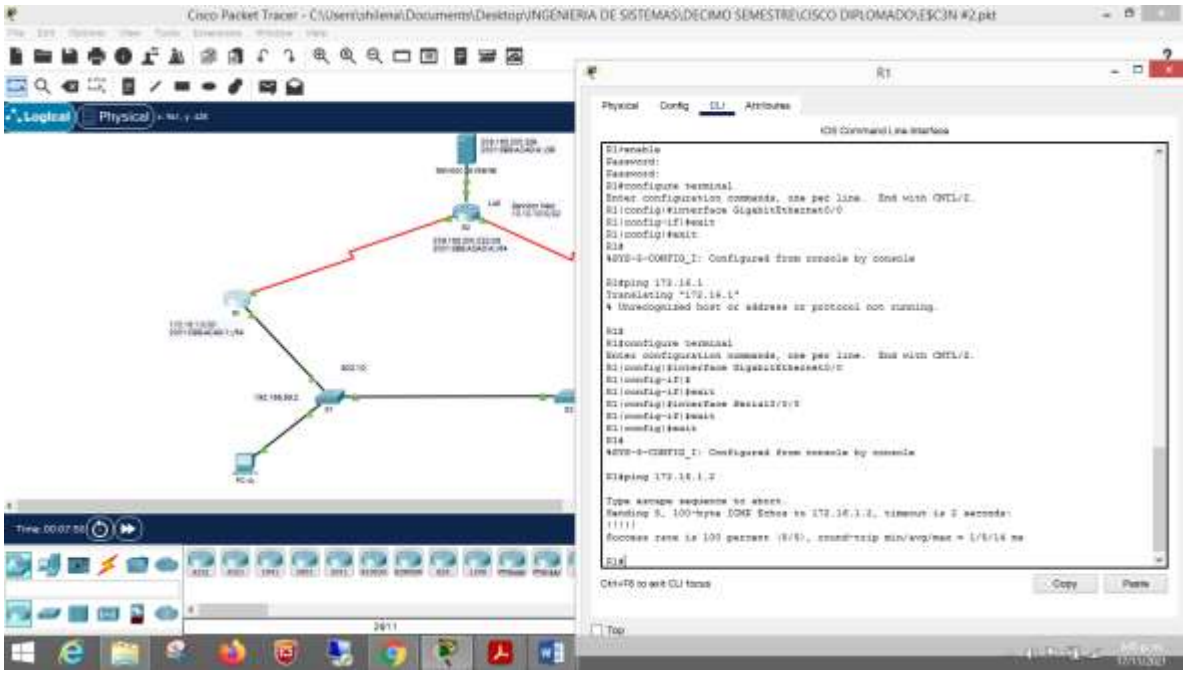
Tabla N. 12 Verificacion conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	R1>enable Password: R1#ping 172.16.1.2 Type escape sequence to abort. 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 = 9/11/13 ms
R2	R3, S0/0/1	172.16.2.1	R2>enable Password: R2#ping 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 = 8/11/13 ms
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data:

			Reply from 209.165.200.233: bytes=32 time=10ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 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 = 10ms, Average = 2ms C:\>

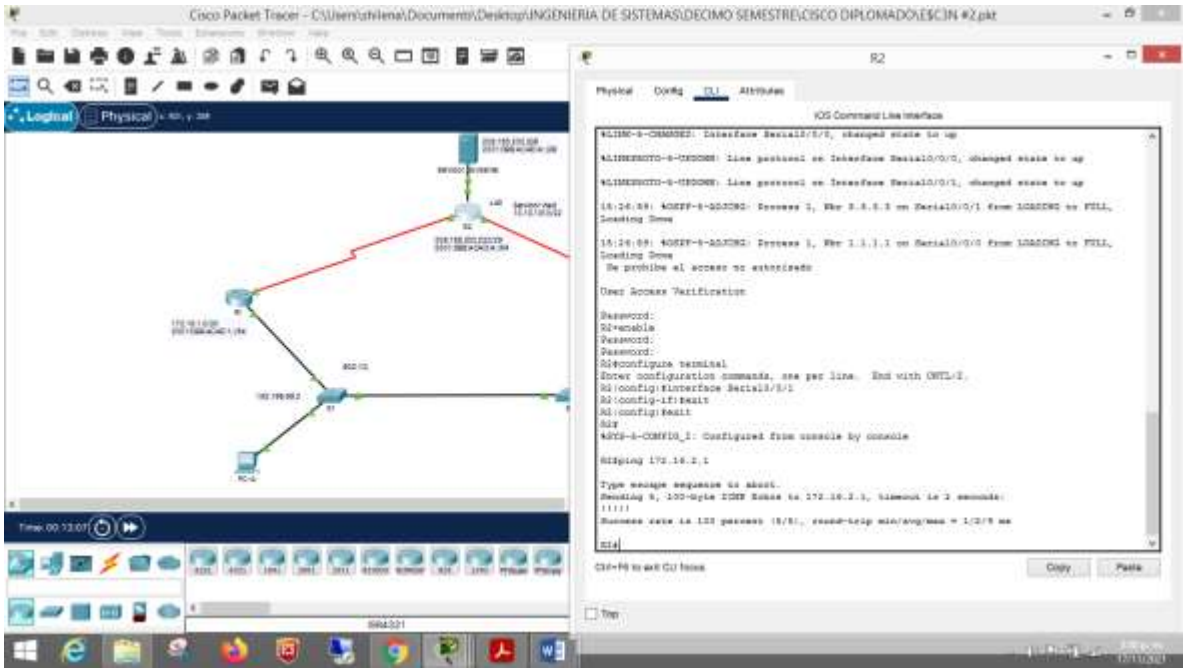
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 18. Verificando conectividad R1



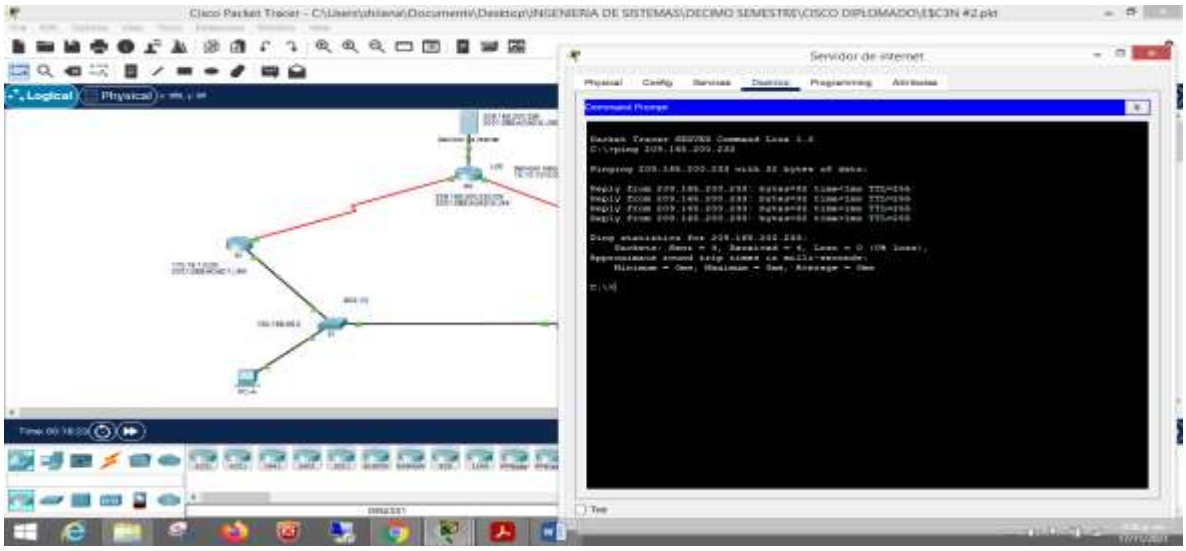
Autoria propia

Figura 19.conectividad R2



Autoria propia

Figura 20. Conectividad servidor internet



Autoria 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:

Tabla N.13 configuracion seguridad S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#**config ter** S1(config)#**vlan 21** S1(config)#**name Contabilidad** S1(config)#**vlan 23** S1(config)#**name Ingenieria** S1(config)#**vlan 99** S1(config)#**name Administracion** S1(config)#**exit** S1#
Asignar la dirección IP de administración.	S1#**config ter** S1(config)#**interface Vlan 99** S1(config)#**ip address 192.168.99.2 255.255.255.0** S1(config)#**no shutdown** S1(config)#**exit** S1#
Asignar el gateway predeterminado	S1#**config ter** S1(config)#**ip default-gateway 192.168.99.1** S1(config)#**exit** S1#
Forzar el enlace troncal en la interfaz F0/3	S1#**config ter** S1(config)#**interface fastEthernet 0/3** S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1** S1(config)#**exit** S1#
Forzar el enlace troncal en la interfaz F0/5	S1#**config t** S1(config)#**interface f0/5** S1(config)#**switchport mode trunk** S1(config)#**switchport trunk native vlan 1**

	S1(config)#**exit** S1#
Configurar el resto de los puertos como puertos de acceso	S1#**config t** S1(config)#**interface range f0/1- 2, f0/4, f0/6-24, g0/1-2** S1(config)#**switchport mode access** S1(config)#**exit** S1#
Asignar F0/6 a la VLAN 21	S1#**config t** S1(config)#**interface f0/6** S1(config)#**switchport access vlan 21** S1(config)#**exit** S1#
Apagar todos los puertos sin usar	S1#**config t** S1(config)#**interface range f0/1- 2, f0/4, f0/7-24, g0/1-2** S1(config)#**shutdown** S1(config)#**exit** S1#

S1>enable
Password:
S1#enable
S1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
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
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#no shutdown

S1(config-if)#exit
S1(config)#int vlan 99
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#int vlan 99
S1(config-if)#no ip default-gateway 192.168.99.1
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#

S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

Figura 21. configuracion seguridad S1

Propia autoria

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:
Tabla N.14 Configuracion S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#**config t** S3(config)#**vlan 21** S3(config)#**name Contabilidad** S3(config)#**vlan 23** S3(config)#**name Ingenieria** S3(config)#**vlan 99** S3(config)#**name Administracion** S3(config)#**exit** S3#
Asignar la dirección IP de administración	S3#**config t** S3(config)#**interface Vlan 99** S3(config)#**ip address 192.168.99.3 255.255.255.0** S3(config)#**no shutdown** S3(config)#**exit** S3#
Asignar el gateway predeterminado.	S3#**config t** S3(config)#**ip default-gateway 192.168.99.1** S3(config)#**exit** S3#
Forzar el enlace troncal en la interfaz F0/3	S3#**config t** S3(config)#**interface f0/3** S3(config)#**switchport mode trunk** S3(config)#**switchport trunk native vlan 1** S3(config)#**exit** S3#
Configurar el resto de los puertos como puertos de acceso	S3#**config t** S3(config)#**interface range f0/1-2, f0/4-24, g0/1-2** S3(config)#**switchport mode access** S3(config)#**exit**

	S3#
Asignar F0/18 a la VLAN 23	S3#**config t** S3(config)#**interface f0/18** S3(config)#**switchport access vlan 23** S3(config)#**exit** S3#
Apagar todos los puertos sin usar	S3#**config t** S3(config)#**interface range f0/1- 2, f0/4-17, f0/19-24, g0/1-2** S3(config)#**shutdown** S3(config)#**exit**

S3>enable
Password:
S3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
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
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access

S3(config-if-range)#exit
S3(config)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

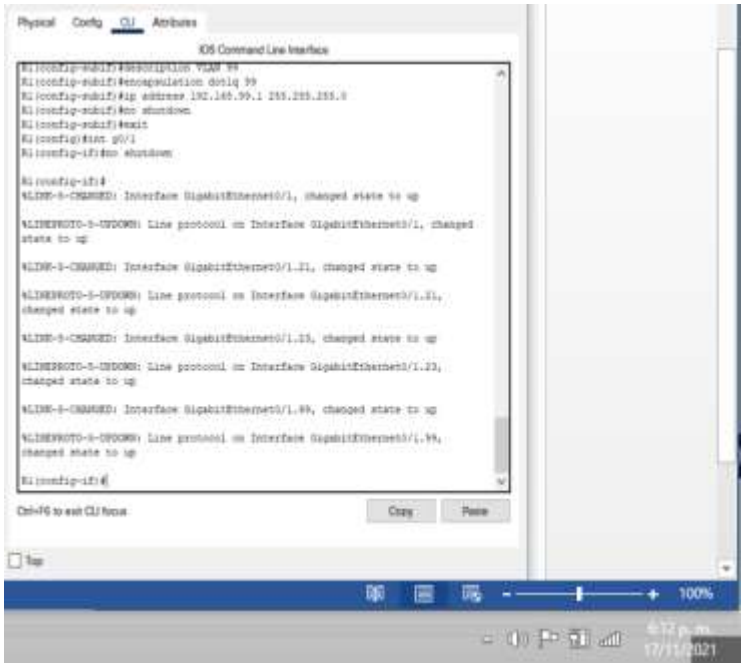
Tabla N.15 configuracion R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#config t R1(config)#**interface gigabitEthernet 0/1.21** R1(config)# **description VLAN 21** R1(config)#**encapsulation dot1Q 21** R1(config)#**ip address 192.168.21.1 255.255.255.0** R1(config)#**no shutdown** R1(config)#**exit** R1#
Configurar la subinterfaz 802.1Q .23 en G0/1	R1#config t R1(config)#**interface gigabitEthernet 0/1.23** R1(config)# **description VLAN 23** R1(config)#**encapsulation dot1Q 23** R1(config)#**ip address 192.168.23.1 255.255.255.0** R1(config)#**no shutdown** R1(config)#**exit** R1#
Configurar la subinterfaz 802.1Q .99 en G0/1	R1#config t R1(config)#**interface gigabitEthernet 0/1.99** R1(config)# **description VLAN 99** R1(config)#**encapsulation dot1Q 99**

	R1(config)#**ip address 192.168.99.1 255.255.255.0** R1(config)#**no shutdown** R1(config)#**exit** R1#
Activar la interfaz G0/1	R1#config t R1(config)#**interface gigabitEthernet 0/1** R1(config)#**no shutdown** R1(config)#**exit** R1#

R1>enable
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#int g0/1.99
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#int g0/1
R1(config-if)#no shutdown

Figura 22. Configuracion R1



Propia autoria

Paso 4: Verificar la conectividad de la red

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

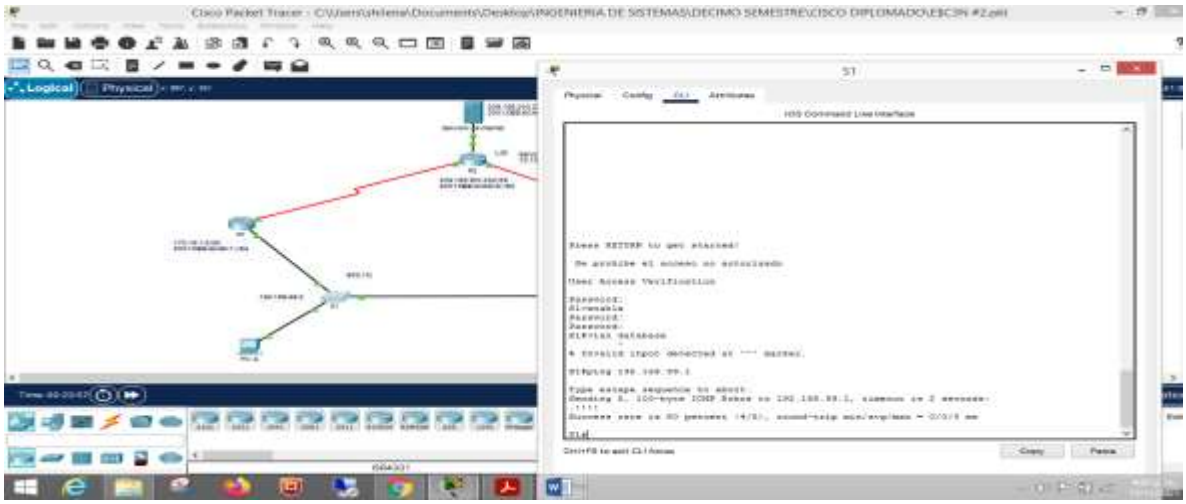
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla N. 16 Verificacion de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1>enable Password: S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

			S1#
S3	R1, dirección VLAN 99	192.168.99.1	S3>enable Password: S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms S3#
S1	R1, dirección VLAN 21	192.168.21.1	S1# S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#

Figura 23.verificacion de conectividad S1



Autoria propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configuraracion OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:
Tabla N. 17 configuracion OSPF R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#config t R1(config)#**router ospf 1** R2(config)#**router-id 1.1.1.1**
Anunciar las redes conectadas directamente	R1(config)#**network 172.16.1.0 0.0.0.3 area 0** R1(config)#**network 192.168.21.0 0.0.0.255 area 0** R1(config)#**network 192.168.23.0 0.0.0.255 area 0** R1(config)#**network 192.168.99.0 0.0.0.255 area 0**
Establecer todas las interfaces LAN como pasivas	R1(config)#**passive-interface g0/1.21** R1(config)#**passive-interface g0/1.23** R1(config)#**passive-interface g0/1.99** R1(config)#**exit** R1#
Desactive la sumarización automática	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R1#config t R1(config)#**router ospf 1** R1(config-router)#**no auto-summary** R1(config-router)#**exit** R1#

Figura 24**.** Configuraracion OSPF en el R1

Propia autoria

R1>enable
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
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
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
^
% Invalid input detected at '^' marker.
R1(config-router)#exit
R1(config)#

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:
Tabla N. 18 configuracion OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#config t R2(config)#**router ospf 1** R2(config)#**router-id 2.2.2.2**
Anunciar las redes conectadas directamente	R2(config)#**network 10.10.10.10 0.0.0.0 area 0** R2(config)#**network 172.16.1.0 0.0.0.3 area 0** R2(config)#**network 172.16.2.0 0.0.0.3 area 0**
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#**passive-interface loopback 0** R2(config)#**exit** R2#
Desactive la sumarización automática.	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R2#config t R2(config)#**router ospf 1** R2(config-router)#**no auto-summary** R2(config-router)#**exit** R2#

R2>enable
Password:
R2#router ospf 1
^
% Invalid input detected at '^' marker.
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
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)#passive-interface loopback 0
R2(config-router)#no auto-summary
^

% Invalid input detected at '^' marker.
R2(config-router)#

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla N.19 Configuración protocolo de enrutamiento en el **R3.**

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#config t R3(config)#**router ospf 1** R3(config)#**router-id 3.3.3.3** R3(config)#
Anunciar redes IPv4 conectadas directamente	R3(config)#**network 172.16.2.0 0.0.0.3 area 0** R3(config)#**network 192.168.4.0 0.0.0.255 area 0** R3(config)#**network 192.168.5.0 0.0.0.255 area 0** R3(config)#**network 192.168.6.0 0.0.0.255 area 0**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config)#**passive-interface loopback 4** R3(config)#**passive-interface loopback 5** R3(config)#**passive-interface loopback 6** R3(config)#**passive-interface loopback 7** R3(config)#**exit** R3#
Desactive la sumarización automática.	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R3#config t R3(config)#**router ospf 1** R3(config-router)#**no auto-summary** R3(config-router)#**exit** R3#

R3>enable
Password:
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
00:19:15: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
net
% Incomplete command.
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
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#passive-interface loopback 7
R3(config-router)#no auto-summary
^
% Invalid input detected at '^' marker.
R3(config-router)#exit
R3(config)#

Paso 4: Verificar la información de OSPF

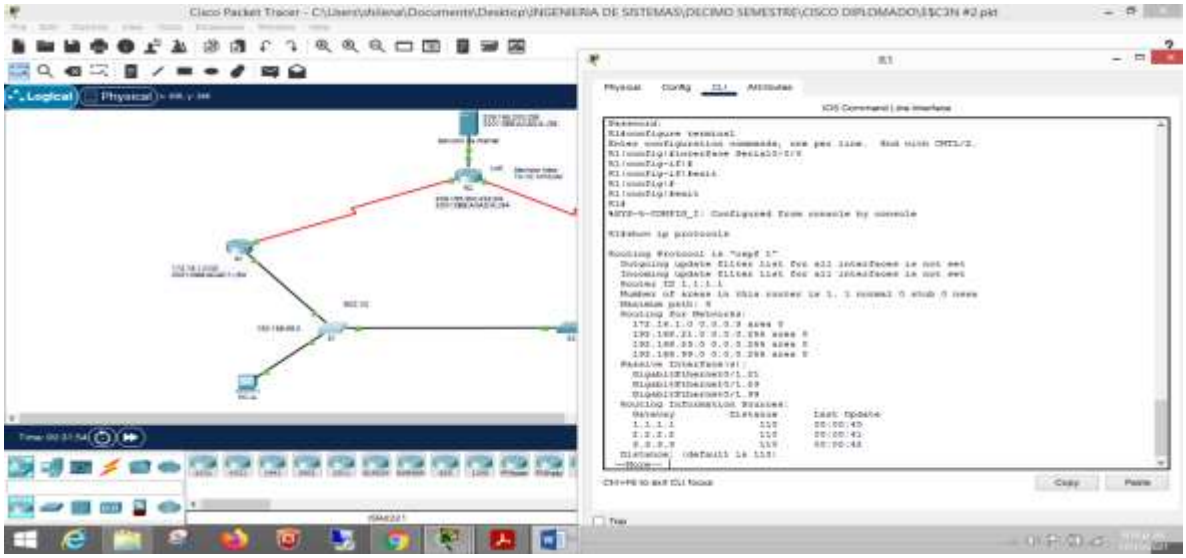
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla N. 20. Verificación 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?	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando: R1#**show ip protocols**

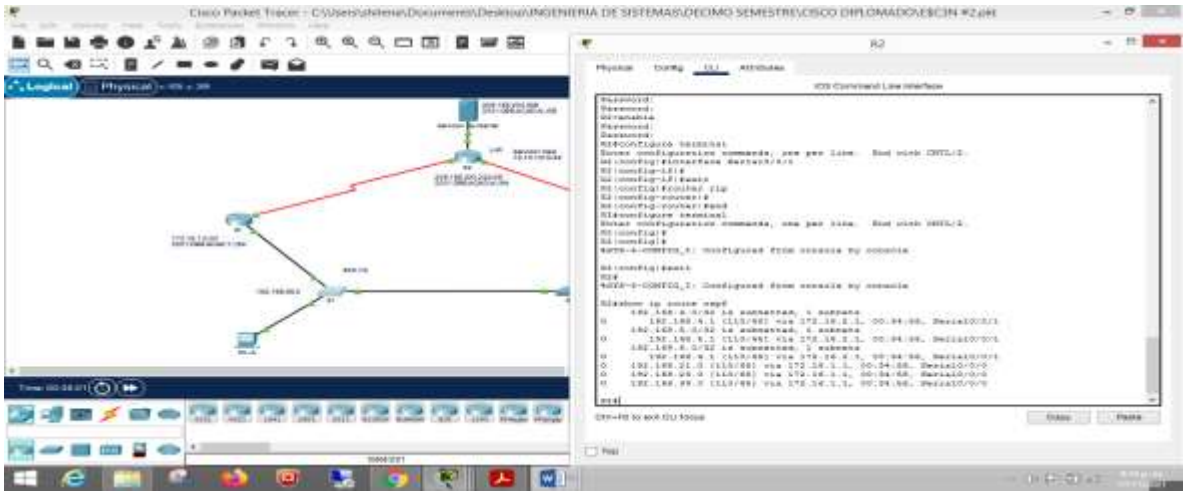
¿Qué comando muestra solo las rutas OSPF?	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando: R2#**show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Desde el modo de usuario y en R1, R2 y R3 se aplica el siguiente comando: R3#**show running-config | section router ospf**

Figura 25.verificacion OSPF en R1



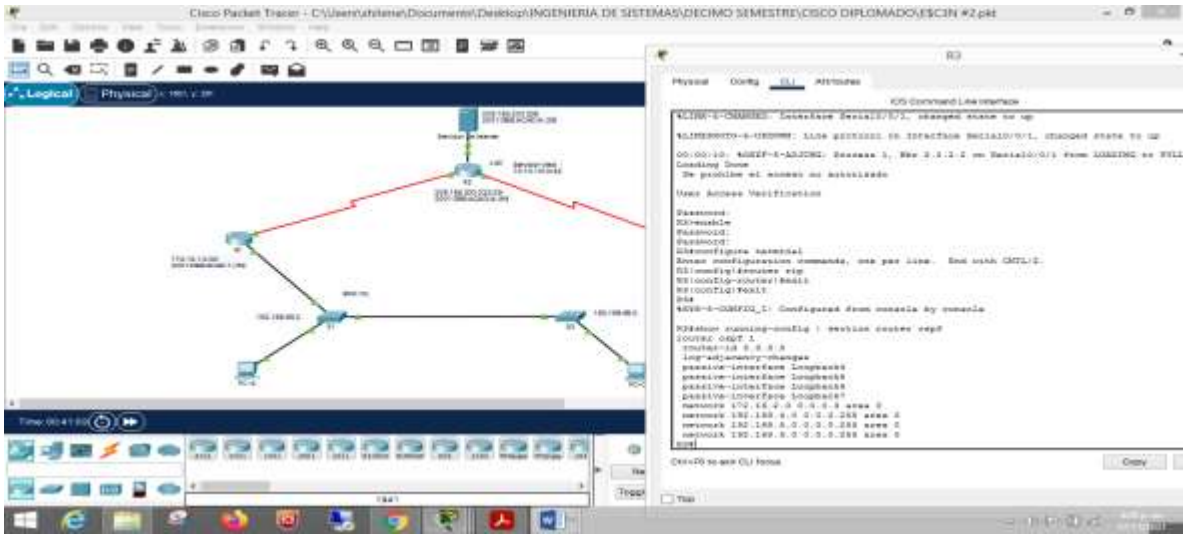
Autoria propia

Figura 26.verificacion OSPF en R2



Autoria propia

Figura 27.verificacion OSPF en R3



Autoria propia.

R1>enable
Password:
R1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1

Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.16.1.0 0.0.0.3 area 0
192.168.21.0 0.0.0.255 area 0
192.168.23.0 0.0.0.255 area 0
192.168.99.0 0.0.0.255 area 0
Passive Interface(s):
GigabitEthernet0/1.21
GigabitEthernet0/1.23
GigabitEthernet0/1.99
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:15:58
2.2.2.2 110 00:09:41
3.3.3.3 110 00:06:52
Distance: (default is 110)

R1#

R2>enable
Password:
R2#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
10.10.10.10 0.0.0.0 area 0
172.16.1.0 0.0.0.3 area 0
172.16.2.0 0.0.0.3 area 0
Passive Interface(s):
Loopback0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:17:24
2.2.2.2 110 00:11:08
3.3.3.3 110 00:08:19
Distance: (default is 110)

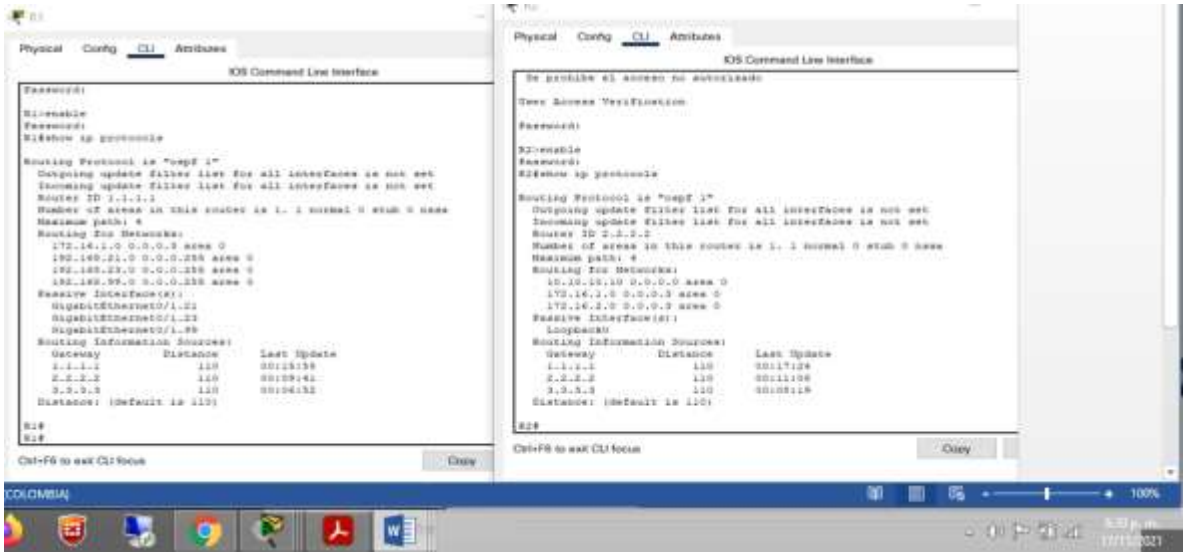
R2#

R3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.16.2.0 0.0.0.3 area 0
192.168.4.0 0.0.0.255 area 0
192.168.5.0 0.0.0.255 area 0
192.168.6.0 0.0.0.255 area 0
Passive Interface(s):
Loopback4
Loopback5
Loopback6
Loopback7
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:18:08
2.2.2.2 110 00:11:52
3.3.3.3 110 00:09:04
Distance: (default is 110)

R3#

Figura 28.verificacion OSPF en R1,R2,R3



Autoria propia

R1#
R1#show ip route ospf

10.0.0.0/32 is subnetted, 1 subnets
O 10.10.10.10 [110/65] via 172.16.1.2, 00:19:39, Serial0/0/0
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.2.0 [110/128] via 172.16.1.2, 00:18:31, Serial0/0/0
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/129] via 172.16.1.2, 00:12:00, Serial0/0/0
192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/129] via 172.16.1.2, 00:11:26, Serial0/0/0
192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/129] via 172.16.1.2, 00:10:31, Serial0/0/0

R1#

R2#show ip route ospf
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/65] via 172.16.2.1, 00:13:59, Serial0/0/1
192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/65] via 172.16.2.1, 00:13:25, Serial0/0/1
192.168.6.0/32 is subnetted, 1 subnets

O 192.168.6.1 [110/65] via 172.16.2.1, 00:12:30, Serial0/0/1
O 192.168.21.0 [110/65] via 172.16.1.1, 00:21:37, Serial0/0/0
O 192.168.23.0 [110/65] via 172.16.1.1, 00:21:37, Serial0/0/0
O 192.168.99.0 [110/65] via 172.16.1.1, 00:21:37, Serial0/0/0

R2#

R3#show ip route ospf
10.0.0.0/32 is subnetted, 1 subnets
O 10.10.10.10 [110/65] via 172.16.2.2, 00:16:23, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.16.1.0 [110/128] via 172.16.2.2, 00:16:23, Serial0/0/1
O 192.168.21.0 [110/129] via 172.16.2.2, 00:16:23, Serial0/0/1
O 192.168.23.0 [110/129] via 172.16.2.2, 00:16:23, Serial0/0/1
O 192.168.99.0 [110/129] via 172.16.2.2, 00:16:23, Serial0/0/1

R3#

R1#show running-config | section router ospf
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
passive-interface GigabitEthernet0/1.21
passive-interface GigabitEthernet0/1.23
passive-interface GigabitEthernet0/1.99
network 172.16.1.0 0.0.0.3 area 0
network 192.168.21.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0
R1#

R2#
R2#show running-config | section router ospf
router ospf 1
router-id 2.2.2.2
log-adjacency-changes

passive-interface Loopback0
network 10.10.10.10 0.0.0.0 area 0
network 172.16.1.0 0.0.0.3 area 0
network 172.16.2.0 0.0.0.3 area 0
R2#

R3#show running-config | section router ospf
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
passive-interface Loopback7
network 172.16.2.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
R3#

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:

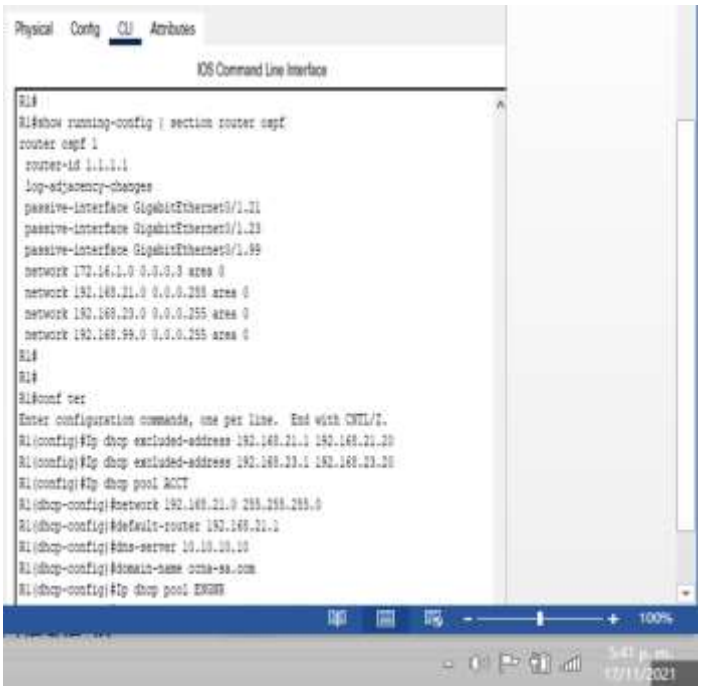
Tabla N. 21. Configuración e implementación DHCP y NAT para IPv4.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#config t R1(config)#**ip dhcp excluded-address 192.168.21.1 192.168.21.20** R1(config)#**exit**

	R1#
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1#config t R1(config)#**ip dhcp excluded-address 192.168.23.1 192.168.23.20** R1(config)#**exit** R1#
Crear un pool de DHCP para la VLAN 21.	R1#config t 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** R1(config)#**exit** R1#
Crear un pool de DHCP para la VLAN 23	R1#config t 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** R1(config)#**exit** R1#

R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#Ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#Ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#Ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#exit
R1(config)#

Figura 29. Configuración e implementación DHCP y NAT para IPv4



Autoria propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla N. 22. Configuración de NAT estática y dinámica en el R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2#config t R2(config)#**username webuser privilege 15 secret cisco12345** R2(config)#**exit** R2#

Habilitar el servicio del servidor HTTP	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http server** R2(config)#**exit** R2#
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	**No aplica** (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#**ip http authentication local** R2(config)#**exit** R2#
Crear una NAT estática al servidor web.	R2#config t R2(config)#**ip nat inside source static 10.10.10.10 209.165.200.237** R2(config)#**exit** R2#
Asignar la interfaz interna y externa para la NAT estática	R2#config t R2(config)#**interface g0/0** R2(config)#**ip nat outside** R2(config)#**interface loopback 0** R2(config)#**ip nat inside** R2(config)#**exit** R2#
Configurar la NAT dinámica dentro de una ACL privada	R2#config t 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** R2(config)#**exit** R2#
Defina el pool de direcciones IP públicas utilizables.	R2#config t R2(config)#**ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248** R2(config)#**exit** R2#

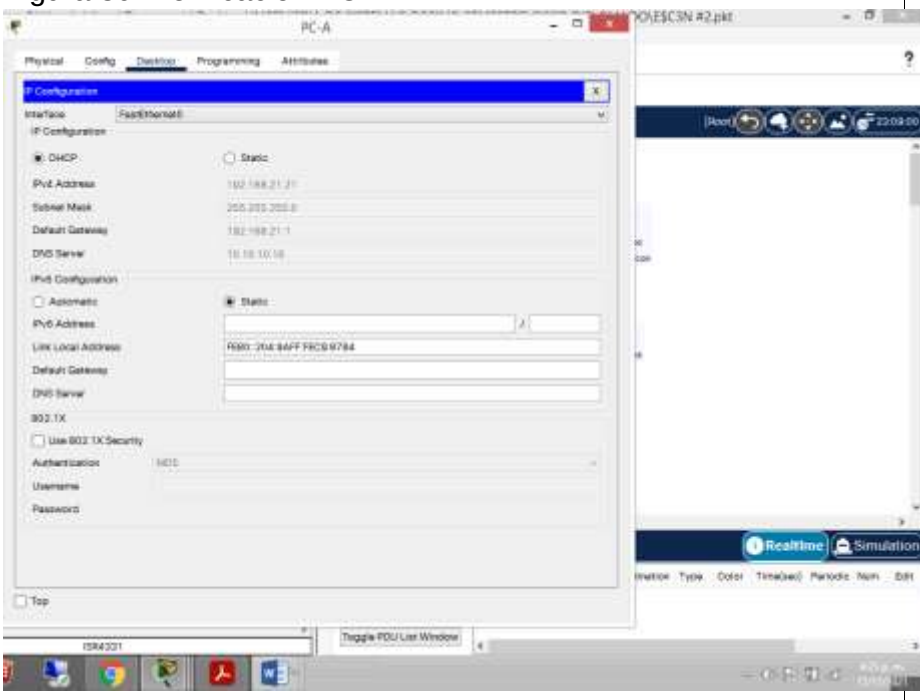
Definir la traducción de NAT dinámica	R2#config t R2(config)#**ip nat inside source list 1 pool INTERNET** R2(config)#**exit** R2#

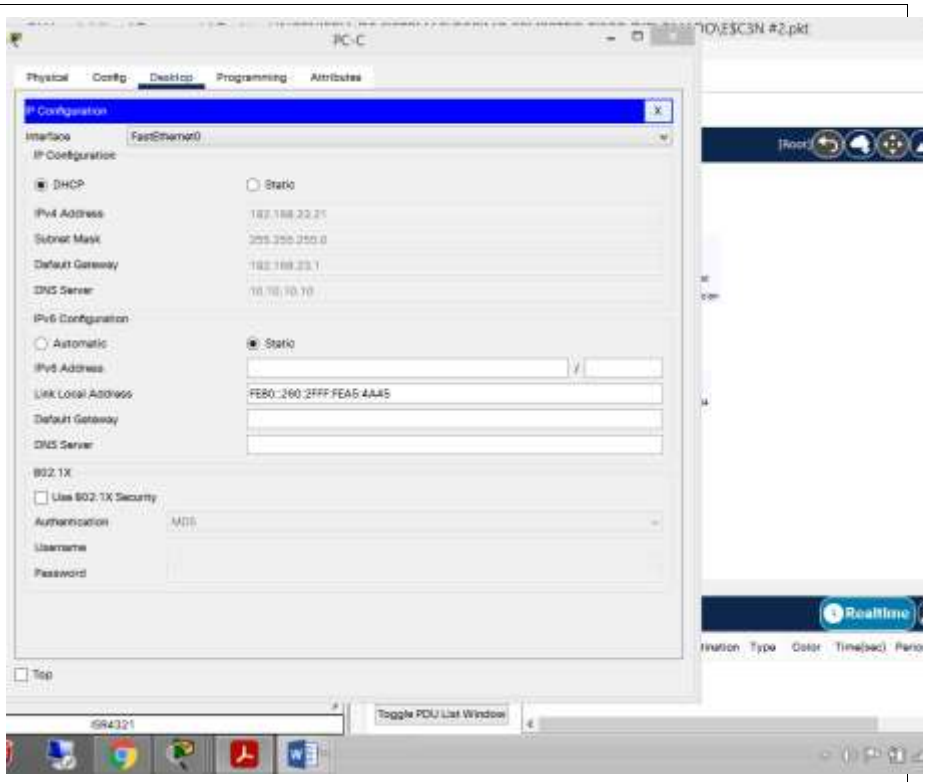
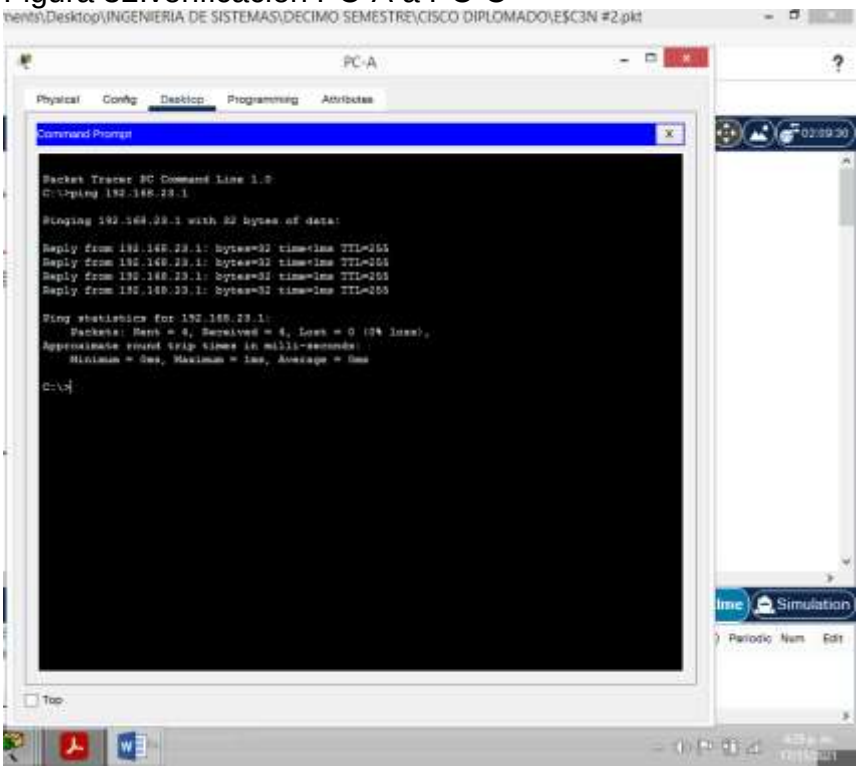
R2>enable
Password:
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
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)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#

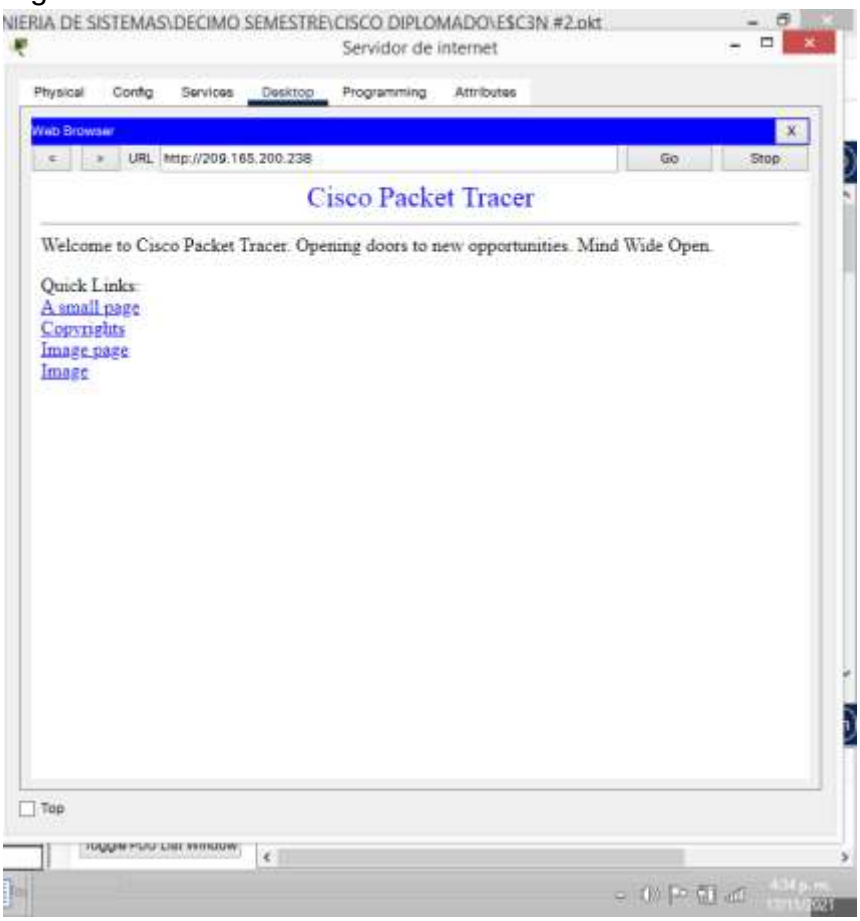
Paso 3: Verificar el protocolo DHCP y la NAT estática

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 N. 23. Verificación de protocolo DHCP y NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ip address 192.168.21.21 Figura 30. Verificación PC-A 
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ip address 192.168.23.21 Figura 31. Verficacion PC-C DHCP

	
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	C:\>ping 192.168.23.21 Figura 32.verificacion PC-A a PC-C 

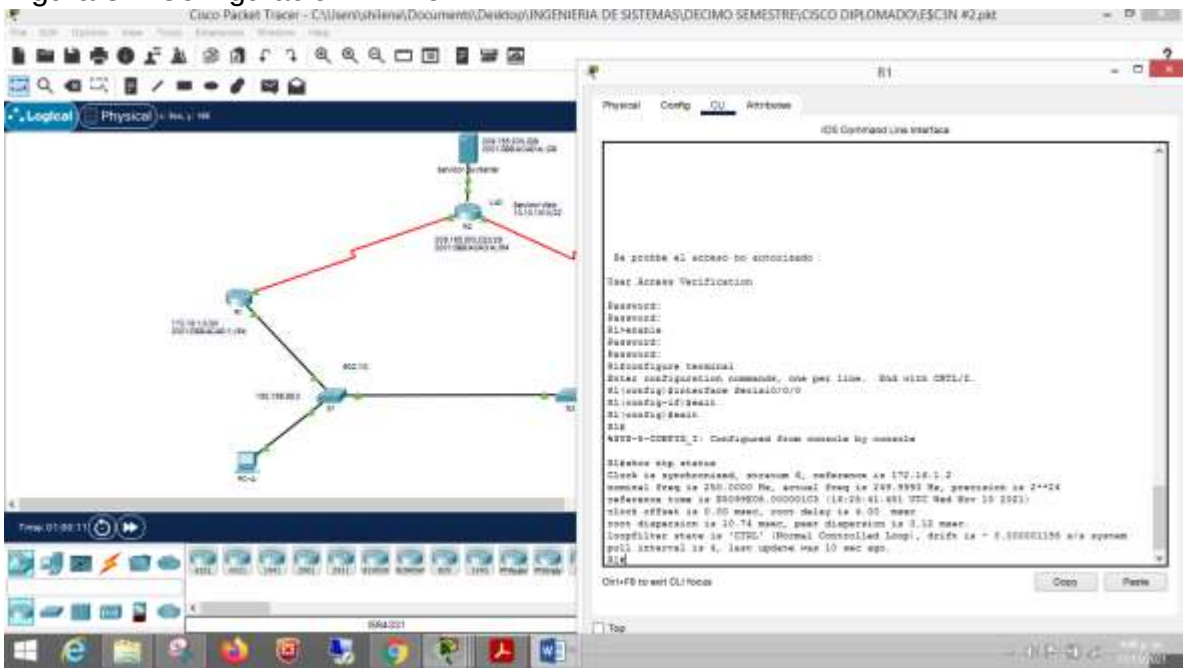
	Pinging 192.168.23.21 with 32 bytes of data: Request timed out. Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	http://209.165.200.237 se aplica en el navegador la IP configurada en el servidor que es: 209.165.200.238 y se visualiza la información configurada en el archivo **index.html** del servidor. Figura 33. Verificando servidor web 

Parte 6: Configurar NTP

Tabla N. 24. Configuración NTP.

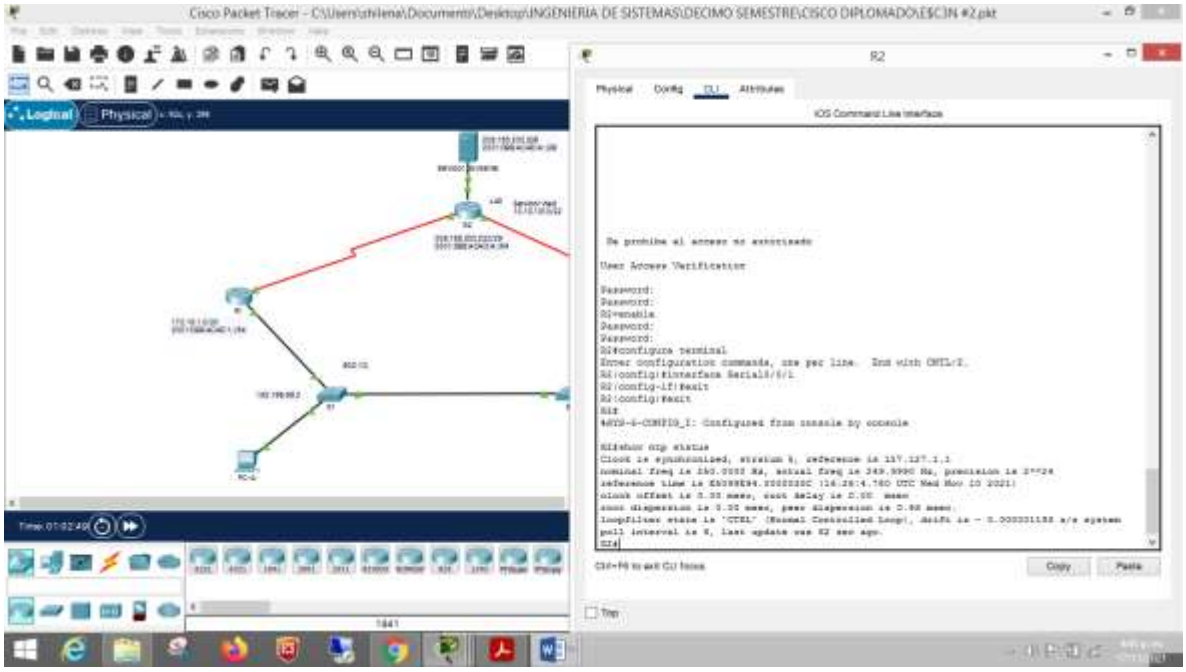
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#**clock set 09:00:00 10 november 2021**
Configure R2 como un maestro NTP.	R2#**config t** R2(config)#**ntp master 5** R2(config)#**exit** R2#
Configurar R1 como un cliente NTP.	R1#config t R1(config)#**ntp server 172.16.1.2** R1(config)#**exit** R1#
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1#config t R1(config)#**ntp update-calendar** R1(config)#**exit** R1#
Verifique la configuración de NTP en R1.	Se aplica el comando **show ntp associations**

Figura 34. Configuración NTP en R1



Propia autoria

Figura 35.Configuración NTP en R2



Propia autoria

R2>enable
Password:
R2#Clock set 14:05:30 10 november 2021
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Ntp master 5
R2(config)#exit
R2#

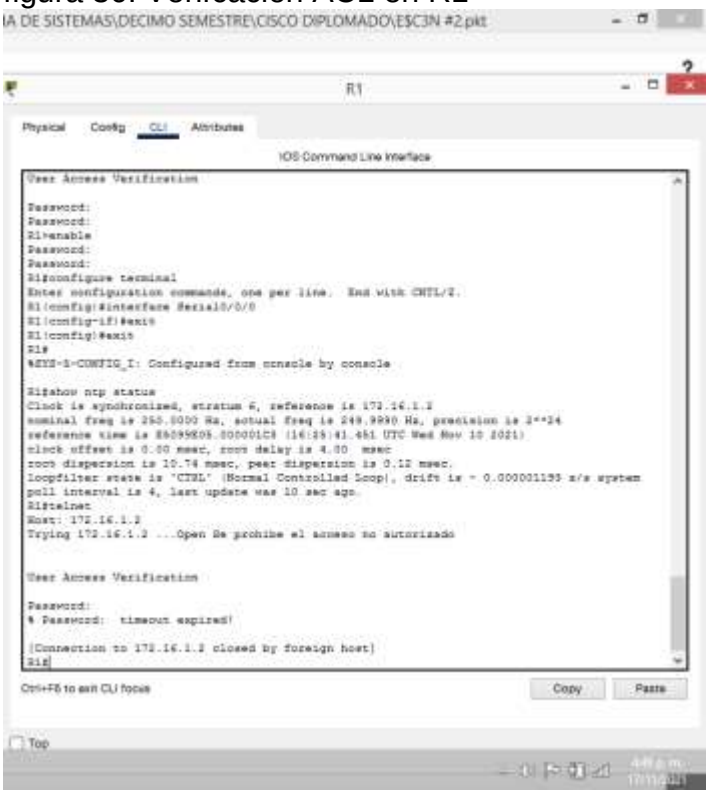
R1>enable
Password:
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#end
R1#

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 N. 25. Restricción de acceso a las líneas VTY en R2.

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

Permitir acceso por Telnet a las líneas de VTY	R2#config t R2(config)#**line vty 0 4** R2(config)#**transport input telnet** R2(config)#**exit** R2#
Verificar que la ACL funcione como se espera	Se aplica en R1 el siguiente comando telnet 172.16.1.2 figura 36. Verifcacion ACL en R1 

R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip Access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
R2(config-line)#exit
R2(config)#

Password:

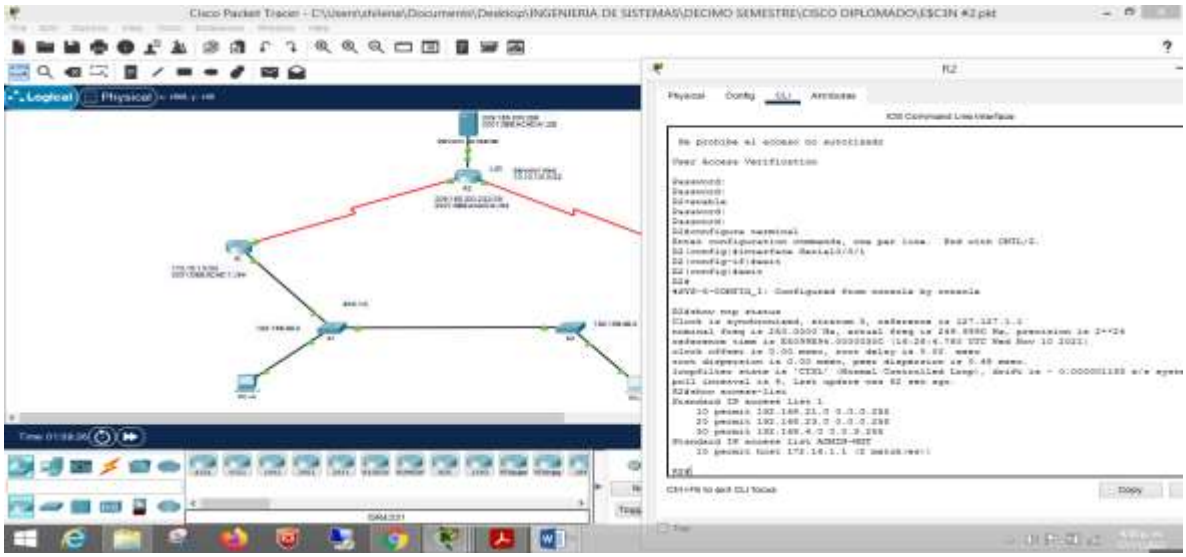
R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado

User Access Verification

Password:
R2>enable
Password:
R2#

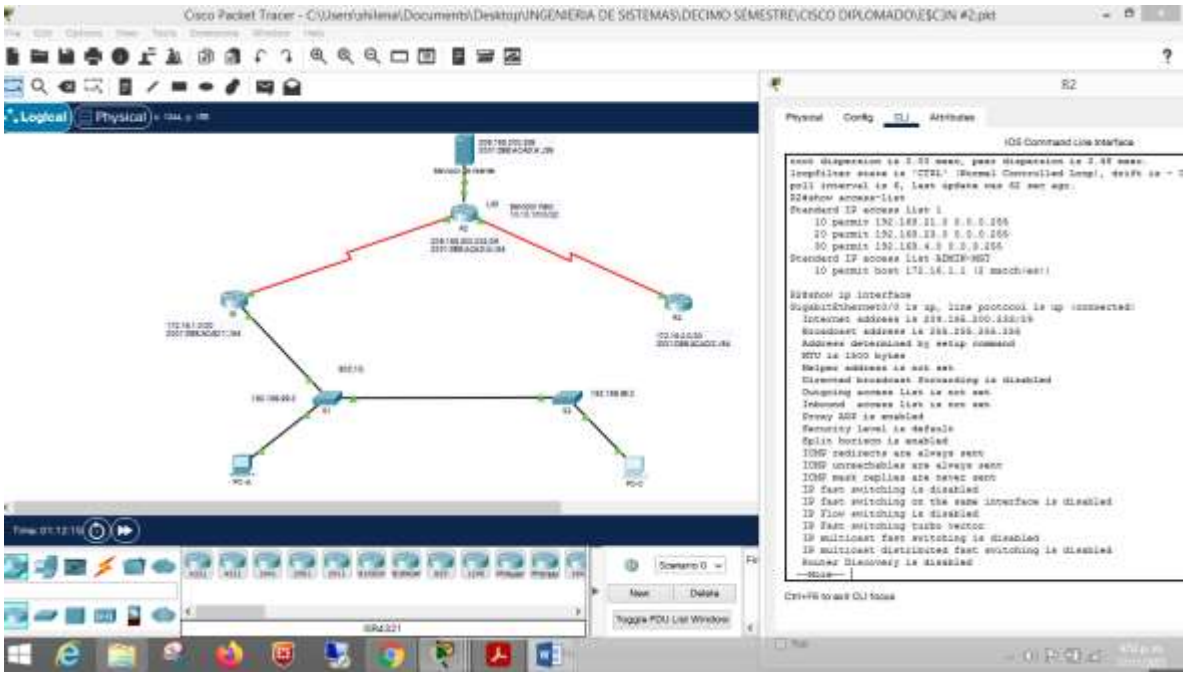
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Figura 37. Verificación comando CLI en R2



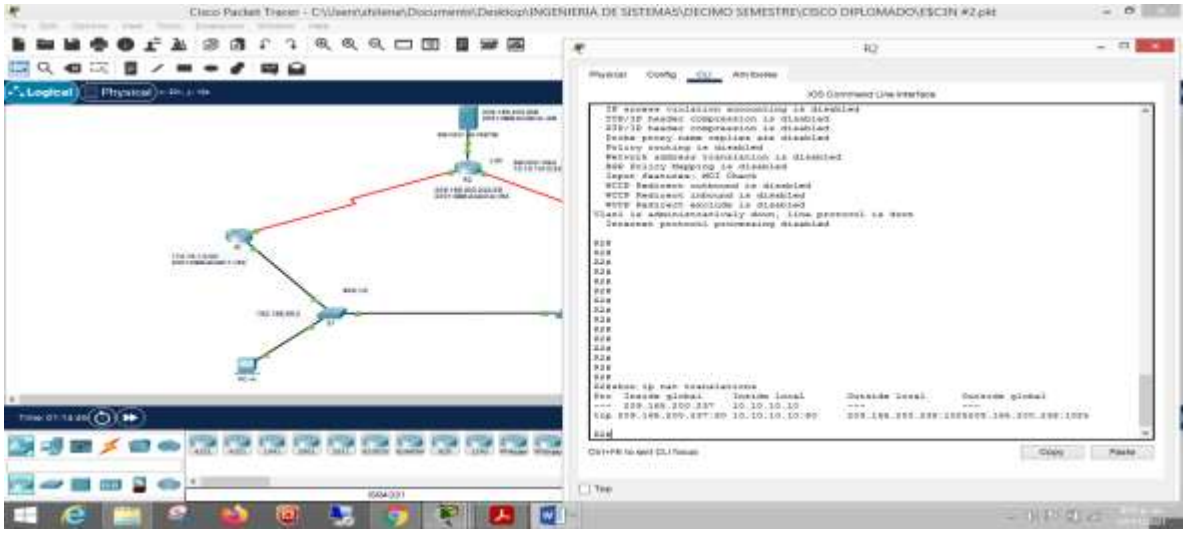
Autoria propia

Figura 38. Verificación comando CLI en R2



Autoria propia

Figura 39. Verificación comando CLI en R2



Autoria propia

Tabla N. 26 Líneas de comando aplicadas a listas de acceso.

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2# **show access-lists**
Restablecer los contadores de una lista de acceso	R2# R2# clear ip access-list counters R2# Obs: Packet tracer no soporta este comando
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2# show ip interface R2#

¿Con qué comando se muestran las traducciones NAT?	R2#**show ip nat translations** **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#**clear ip nat translation**

CONCLUSIONES

Es muy importante esta practica que nos ofrece el diplomado CISCO, los dos escenarios son una práctica exigente que permite atender diferentes temáticas y focaliza su estudio hacia el análisis, investigación y desarrollo que genera habilidades y destrezas en el diseño e implementación de una red. Dentro de las temáticas, se hizo necesario profundizar sobre EtherChannel, protocolo LACP, OSPF, NAT y ACL.

Una gran satisfacion por lograr los objetivos donde se logro la conexión, configuración y simulación de los dispositivos de las redes en los correspondientes escenarios.

BIBLIOGRAFIA

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

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

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

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

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

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