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

GUSTAVO ADOLFO RIOS AYALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

COROZAL

2021

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

GUSTAVO ADOLFO RIOS AYALA

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

DIRECTOR /TUTOR

JAVIER RICARDO VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

COROZAL

2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Corozal, (noviembre 28, 2021)

DEDICATORIA

Primero que todo va dedicado a Dios que es el ser supremo del universo, quién nos da la vida, salud y sobre todo nos llena de sabiduría para avanzar y cumplir nuestros propósitos, segundo a mis padres, mi esposa y suegra que día a día siempre están apoyándome moralmente, siendo ellos el motor principal para nunca rendirme y cumplir con éxito los objetivos propuestos en mi vida.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar presente, en todos los momentos y ser mi guía incondicional.

De igual forma a la Universidad Nacional Abierta y a Distancia – UNAD. A toda la Escuela De Ciencias Básicas, Tecnología E Ingeniería y profesores quienes con sus conocimientos, experiencias y apoyo incondicional contribuyeron a mi crecimiento personal y profesional.

En especial quiero agradecer de todo corazón a la Compañía Desminado Humanitario de la Armada de Colombia, por brindarme la oportunidad, apoyo y flexibilidad para ingresar a la universidad, desarrollar y culminar con éxito la carrera profesional en Ingeniería de Sistema.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

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.

En cuanto al escenario 2, se evalúan las competencias en la implementación del enrutamiento donde se realiza diferentes procesos como es el habilitar y deshabilitar DNS, al igual que VLAN. Se identifica las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP.

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 for scenario 2, the competencies in the implementation of routing are evaluated where different processes are carried out, such as enabling and disabling DNS, as well as VLAN. It identifies the monitoring tools and network management protocols available in the IOS to solve data network problems, evaluating the performance of routers and switches, through the use of specialized commands in network management and compatible with the SMNP protocol.

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 de 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.

OBJETIVOS

General

Desarrollar los escenarios propuestos en el Diplomando de Profundización CISCO aplicando las competencias y habilidades desarrolladas durante el proceso académico dando respuesta y solución a cada uno de estos.

Específicos

- Diseñar, instalar, configurar y administrar redes conmutadas.
- 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.
- Resolver problemas de red relacionados con; Administración, Seguridad y Escalabilidad en redes conmutadas.
- Aprender a realizar resolución de problemas en problemas de enrutamiento avanzados.

DESARROLLO DE LOS ESCENARIOS

1. Escenario 1

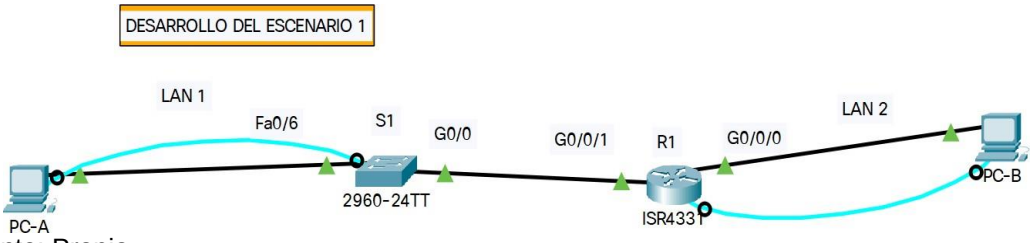
figura 1. Topología escenario 1

Fuente: Propia

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.

Parte 1: Construcción de la red

figura 2. Construcción de la red



Fuente: Propia

Se realizó la implementación de la topología en el simulador cisco Packet Tracer, con el fin de realizar la respectiva configuración.

Parte 2: Desarrolle el esquema de direccionamiento IP

Se realizó el desarrolle del esquema de direccionamiento IP, para la dirección IPv4 se crea las dos subredes con la cantidad requerida de hosts. Se asigno las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1. Direccionamiento

<table>
<tr><th>Item</th><th>Requerimiento</th></tr>
<tr><td>Dirección de Red</td><td>192.168.64.0 donde 64 corresponde a los últimos dos dígitos de su cédula.</td></tr>
<tr><td>Requerimiento de host Subred LAN1</td><td>100
<table><tr><th>dirección de red</th><th>primera ip asignable</th><th>ultima ip asignable</th><th>dirección de broadcast</th></tr><tr><td>192.168.64.0/25</td><td>192.168.64.1/25</td><td>192.168.64.126/25</td><td>192.168.64.127/25</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>dirección de red</th><th>primera ip asignable</th><th>ultima ip asignable</th><th>dirección de broadcast</th></tr><tr><td>192.168.64.128/26</td><td>192.168.64.129/26</td><td>192.168.64.190/26</td><td>192.168.64.191/26</td></tr></table>Mascara de subred
255.255.255.192</td></tr>
<tr><td>R1 G0/0/1</td><td>Primera dirección de host de la subred LAN1
192.168.64.1/25</td></tr>
<tr><td>R1 G0/0/0</td><td>Primera dirección de host de la subred LAN2
192.168.64.129/26</td></tr>
<tr><td>S1 SVI</td><td>Segunda dirección de host de la subred LAN1
192.168.64.2/25</td></tr>
<tr><td>PC-A</td><td>Última dirección de host de la subred LAN1
192.168.64.126/25</td></tr>
<tr><td>PC-B</td><td>Última dirección de host de la subred LAN2
192.168.64.190/26</td></tr>
</table>

Fuente: Propia

Parte 3: Configure aspectos básicos

Se realiza en los dispositivos de red (S1 y R1) la configuración mediante conexión de consola.

Paso 1: Configuración de los ajustes básicos.

Se realizo la configuración para R1 realizando el siguiente proceso:

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**
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**

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-if)#**description Vlan2 Bikes** R1(config-if)#**ip address** 192.168.64.129 **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-if)#**description Vlan2 Bikes** R1(config-if)#**ip address** 192.168.64.1 **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#

Fuente: Propia

Se realizo la configuración de R1 en la topología implementada en el simulador, donde se realizó cada uno de los pasos y configuración sugerida, como se muestra a continuación;

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 192.168.64.129 255.255.255.192

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 192.168.64.1 255.255.255.128

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]

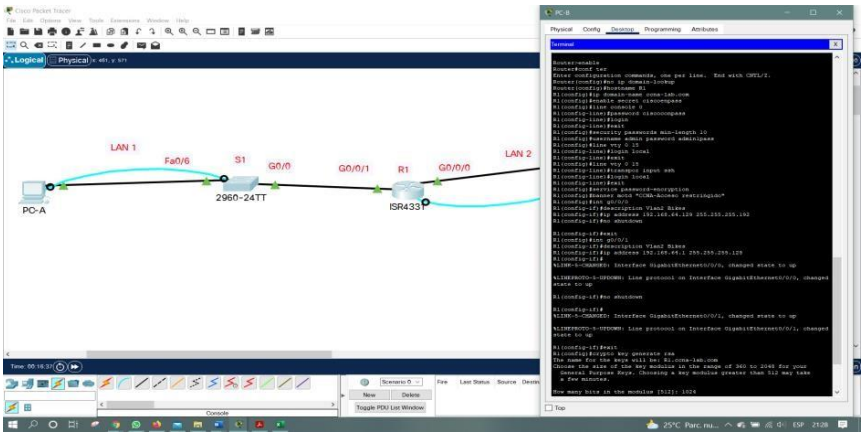
R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console

R1#

figura 3 configuración R1 por medio de consola



Fuente: Propia

Se realizó la configuración de S1 realizando el siguiente proceso:

Tabla 3. 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)#**transport input ssh** 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 Vlan1**
Configuración del gateway predeterminado	S1(config)# S1(config)#**ip default-gateway** 192.168.64.2 S1(config)#**do wr** Building configuration... [OK] S1(config)#

Fuente: Propia

Se realizó la configuración de R1 en la topología implementada en el simulador, donde se realizó cada uno de los pasos y configuración sugerida.

Switch>enable

Switch#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup

Switch(config)#hostname S1

S1(config)#ip domain-name ccna-lab.com

S1(config)#enable secret ciscoenpass

S1(config)#line console 0

S1(config-line)#password ciscoconpass

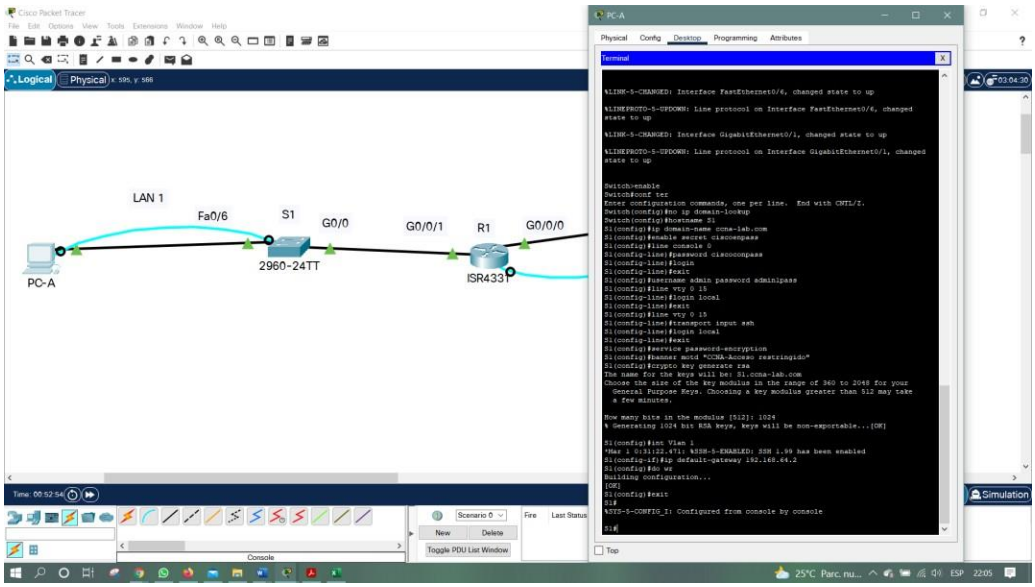
S1(config-line)#login

S1(config-line)#exit

S1(config)#username admin password admin1pass

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "CCNA-Acceso restringido"
S1(config)#crypto key generate rsa
The name for the keys will be: S1.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]
S1(config)#int Vlan 1
*Mar 1 0:31:22.471: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip default-gateway 192.168.64.2
S1(config)#do wr
Building configuration...
[OK]
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

figura 4 configuración S1 por consola



Fuente: Propia

Paso 2. Configurar los equipos

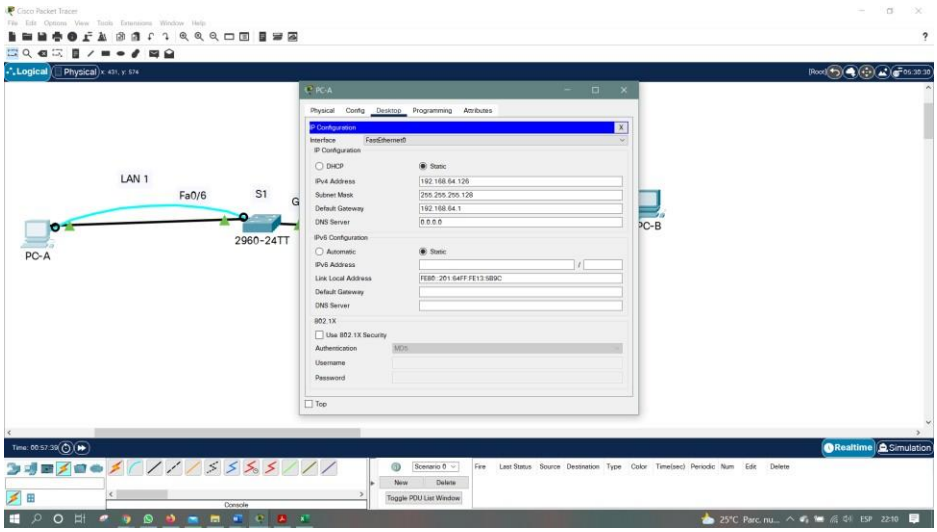
Se realizó la Configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, así mismo se la configuración de red del host con el comando **ipconfig /all**

Tabla 4 Configuración de los equipos host PC-A.

PC-A Network Configuration	
Descripción	**PC-A**
Dirección física	192.168.64.0
Dirección IP	192.168.64.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.64.1

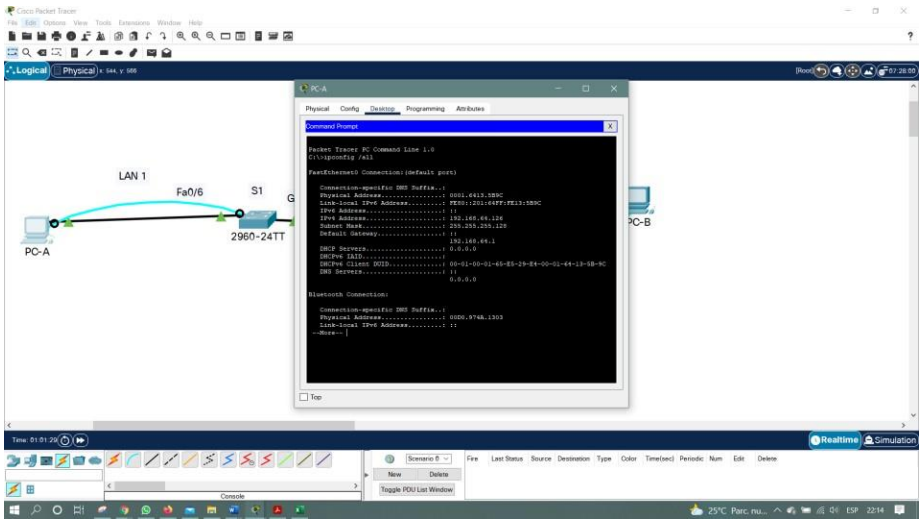
Fuente: Propia

figura 5 configuración PC-A



Fuente: Propia

figura 6 verificación comando **ipconfig /all** en la PC-A



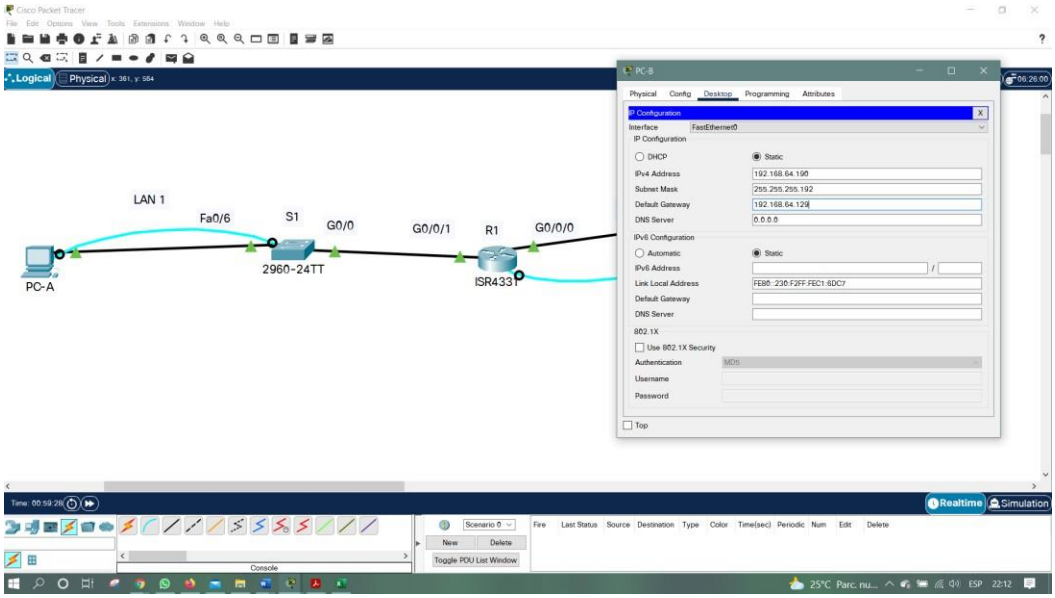
Fuente: Propia

Tabla 5 Configuración de los equipos host PC-B.

PC-B Network Configuration	
Descripción	**PC-B**
Dirección física	192.168.64.128
Dirección IP	192.168.64.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.64.129

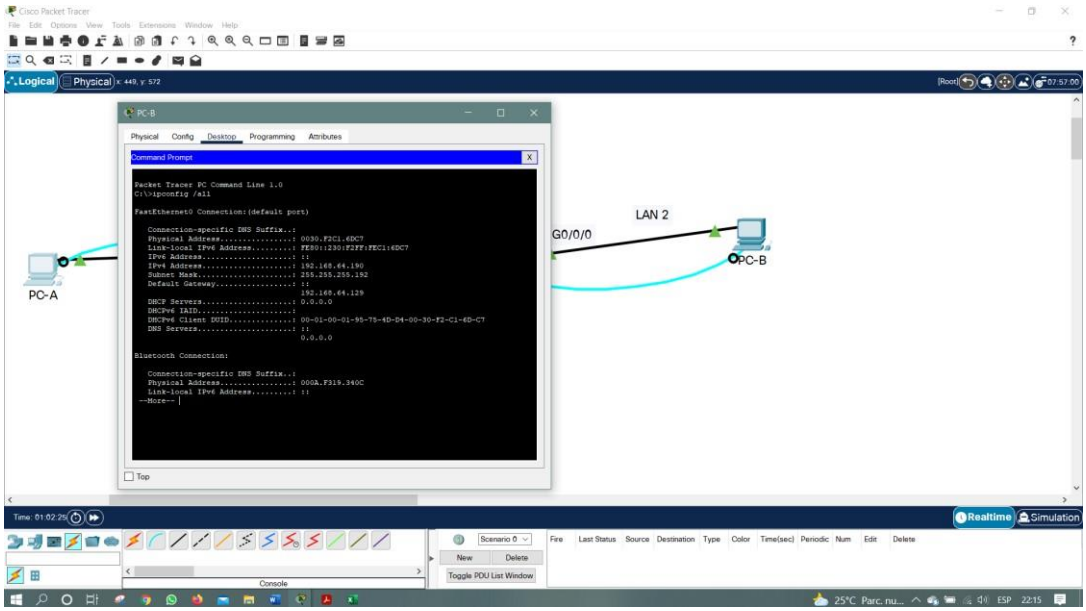
Fuente: Propia

figura 7 configuración PC-B



Fuente: Propia

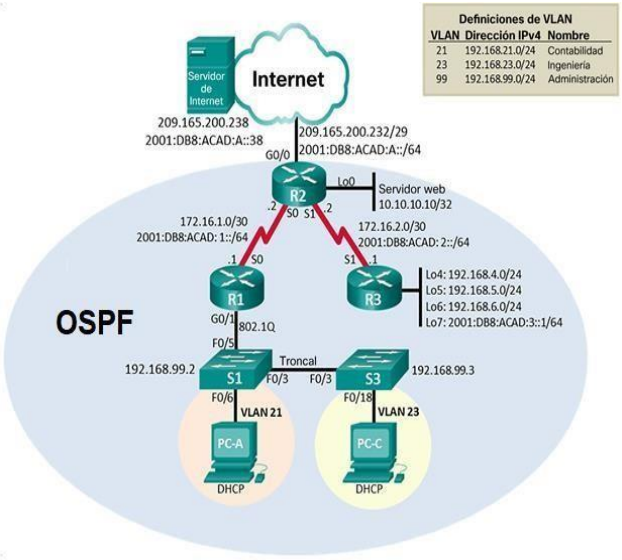
figura 8 verificación comando **ipconfig /all** en la PC-B



Fuente: Propia

2. Escenario 2

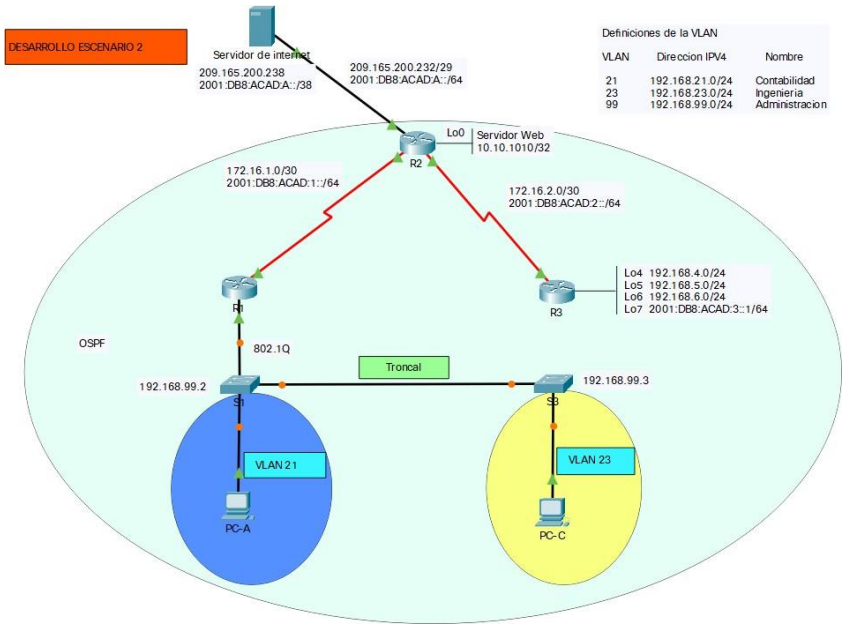
figura 9. Topología escenario 2



Fuente: Propia

Parte 1: Inicializar dispositivos

figura 10. Construcción de la red simulador Packet Tracer



Fuente: Propia

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

Se realizó los pasos de eliminación de las configuraciones de inicio y se vuelven a cargar los dispositivos.

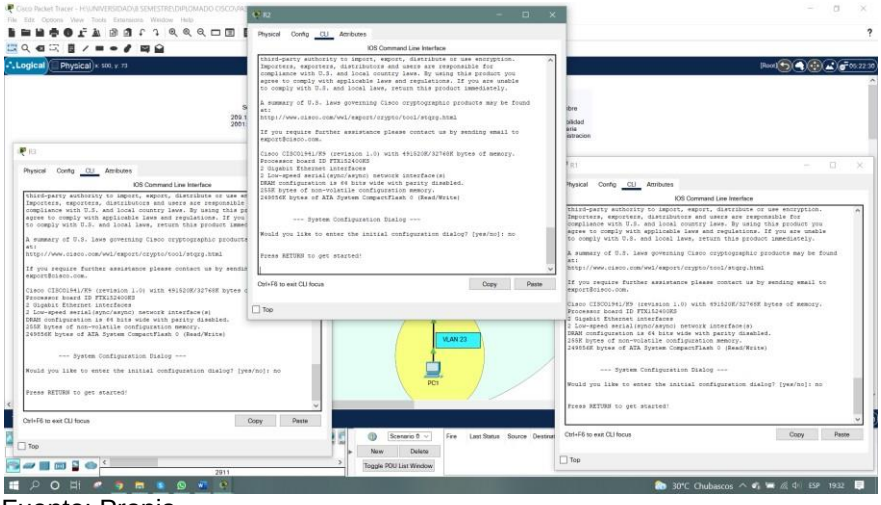
Tabla 6. Pasos para iniciar y cargar los routers y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Routers **R1, R2 y R3** Router>**enable** Router# **erase startup-config**
Volver a cargar todos los routers	Routers **R1, R2 y R3** Router# **reload**
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switches **S1 y S2** Switch# **erase startup-config** Switch# **delete vlan.dat**
Volver a cargar ambos switches	Configuración Switches **S1 y S2** Switch# **reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#**show vlan brief**

Fuente: Propia

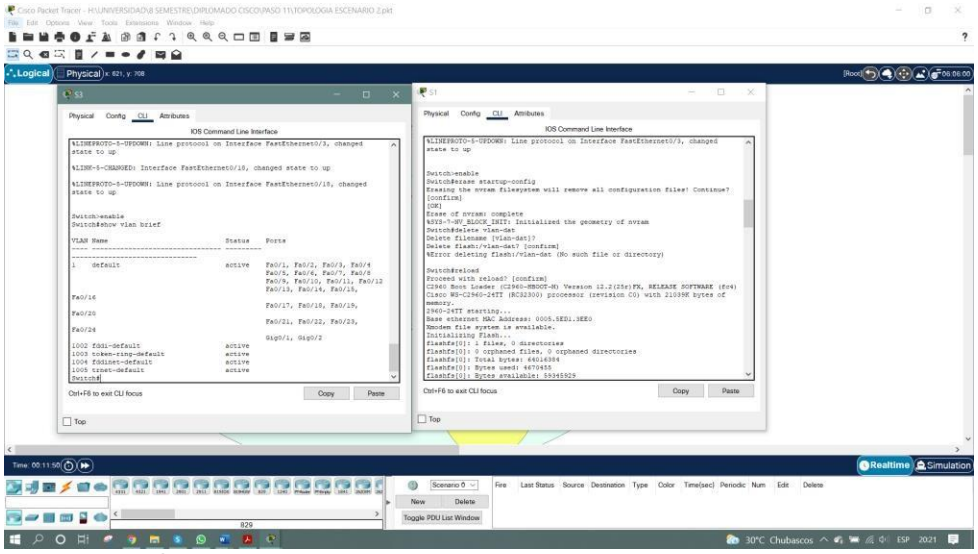
Se realizó los respectivos pasos de eliminación y cargue de los dispositivos de acuerdo con los comandos de IOS de la tabla 6, estos pasos se evidencian a continuación.

figura 11. configuraciones de inicio y cargar de los router.



Fuente: Propia

figura 12. configuraciones de inicio y cargar de los Switches.



Fuente: Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Se verifico la red de la computadora del servidor de internet obteniendo el siguiente resultado como se muestra en la tabla 7.

Tabla 7. Direcciones IP acuerdo la topología.

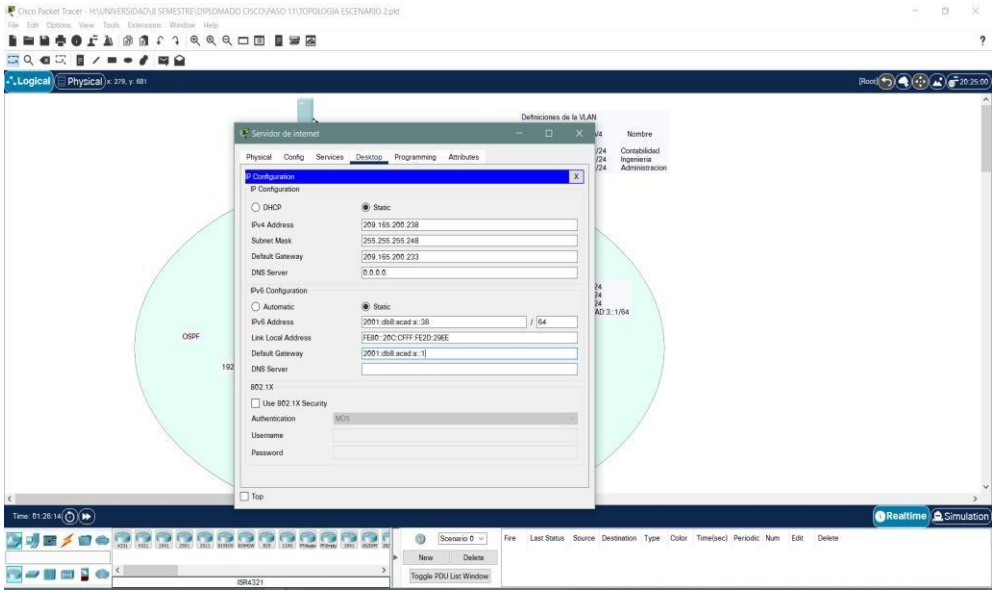
Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Propia

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.

Se realizó la configuración de la computadora del servidor de internet como se muestra a continuación en la figura 13.

figura 13. Configuración de la computadora servidor.



Fuente: Propia

Paso 2: Configurar R1

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración el R1 como se especifica a continuación en la tabla 8.

Tabla 8. Pasos para configuración 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**

Fuente: Propia

Nota: Todavía no configure G0/1.

Se realizó la configuración en R1 de acuerdo con la tabla 8, donde se configuro la seguridad de acceso, configuración de las interfaces y su ruta predeterminada como se evidencia a continuación.

```
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

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración el R2 como se especifica a continuación en la tabla 9.

Tabla 9. Pasos para configuración 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#

Fuente: Propia

Se realizó la configuración en R2 acuerdo especificaciones en la tabla 9, donde se configuro la seguridad de acceso, configuración de las interfaces y su ruta predeterminada como se evidencia a continuación.

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

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración el R3 como se especifica a continuación en la tabla 10.

Tabla 10. Pasos para configuración 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#

Fuente: Propia

Se realizó la configuración en R3 acuerdo especificaciones en la tabla 10, donde se configuro la seguridad de acceso, configuración de las interfaces y su ruta predeterminada como se evidencia a continuación.

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)#

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3(config-if)#exit

R3(config)#int loopback 4

R3(config-if)#ip address 192.168.4.1 255.255.255.0

%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

R3(config-if)#int loopback 5

R3(config-if)#ip address 192.168.5.1 255.255.255.0

%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

R3(config-if)#int loopback 6

R3(config-if)#ip address 192.168.6.1 255.255.255.0

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

R3(config-if)#int loopback 7

R3(config-if)#ipv6 address 2001:db8:acad:3::1/64

%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

R3(config-if)#

R3(config-if)#exit

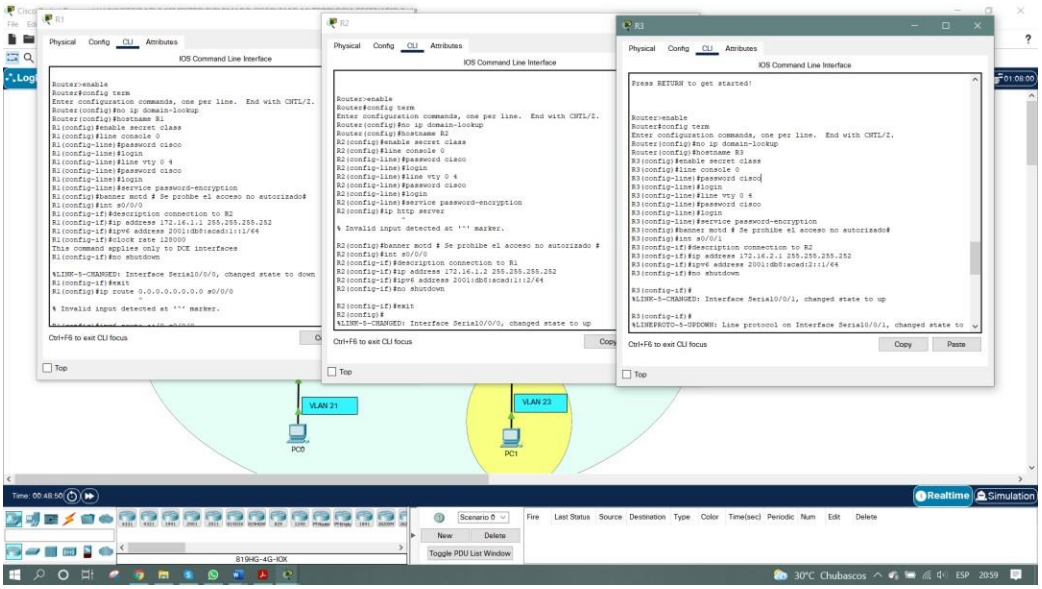
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

%Default route without gateway, if not a point-to-point interface, may impact performance

R3(config)#ipv6 route ::/0 s0/0/1

R3(config)#

figura 14. Configuración de R1, R2 y R3.



Fuente: Propia

Paso 5: Configurar S1

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración de S1 como se especifica a continuación en la tabla 11.

Tabla 11. Pasos para configuración 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#

Fuente: Propia

Se realizó la configuración en S1 acuerdo especificaciones en la tabla 11, donde se configuro la seguridad de acceso, como se evidencia a continuación.

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

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración de S3 como se especifica a continuación en la tabla 12.

Tabla 12. Pasos para configuración 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#

Fuente: Propia

Se realizó la configuración en S3 acuerdo especificaciones en la tabla 12, donde se configuro la seguridad de acceso, como se evidencia a continuación.

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

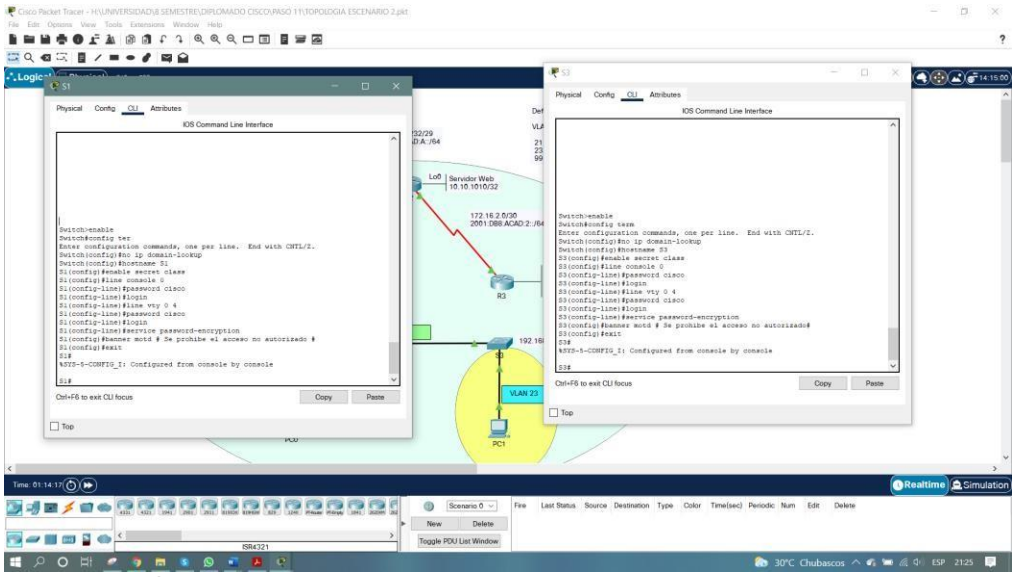
S3(config-line)#service password-encryption

S3(config)#banner motd # Se prohibe el acceso no autorizado#

S3(config)#exit

S3#

figura 15. Configuración de S1 y S3



Fuente: Propia

Paso 7: Verificar la conectividad de la red.

Se utilizo el comando **ping** para probar la conectividad entre los dispositivos de red, verificando metódicamente la conectividad con cada dispositivo de red.

Tabla 13. Resultado de ping.

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.

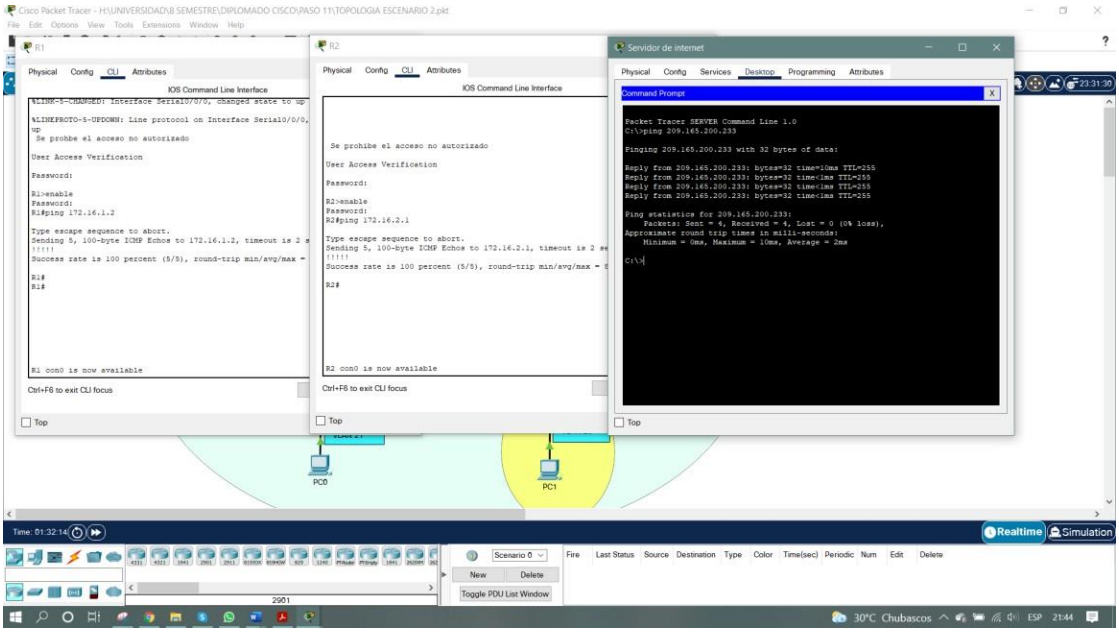
			Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 9/11/13 ms
R2	R3, S0/0/1	172.16.2.1	R2>enable Password: R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/13 ms
PC de Internet	Gateway predeterminado Fuente: Propia	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:\>

Fuente: Propia

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

Se realizó la comprobación a cada uno de los dispositivos, con el fin de verificar la conectividad dando como resultado ping exitosos.

figura 16. Resultado de la ejecución del comando ping.



Fuente: Propia

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

Paso 1: Configurar S1

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración de S1 como se especifica a continuación en la tabla 14.

Tabla 14. Comandos para configuras 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#

Fuente: Propia

Se realizó la configuración en S1 acuerdo especificaciones en la tabla 14, donde se configuro las Vlan y la interfaz de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

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

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

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S1(config-if-range)#exit

S1(config)#

S1#

Paso 2: Configurar el S3

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración de S3 como se especifica a continuación en la tabla 15.

Tabla 15. Comandos para configuras S1.

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**

Fuente: Propia

Se realizó la configuración en S3 acuerdo especificaciones en la tabla 15, donde se configuro las Vlan y la interfaz de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

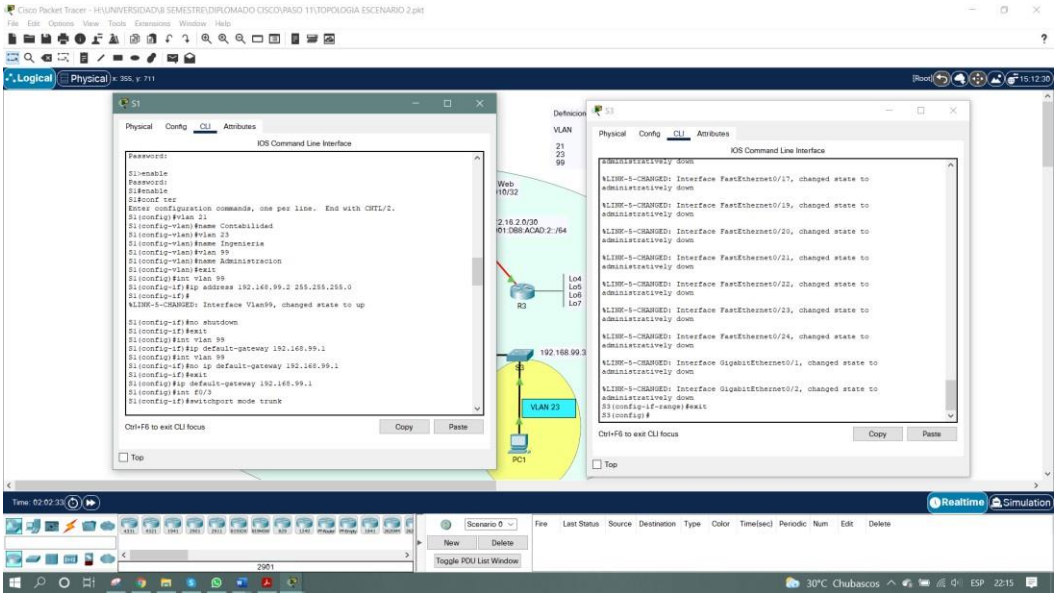
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

S3(config-if-range)#exit

S3(config)#

figura 17. Configuración de S1 y S3



Fuente: Propia

Paso 3: Configurar R1

Se realizó la tabla con cada uno de los comandos que se utilizó en la configuración de R1 como se especifica a continuación en la tabla 16.

Tabla 16. Comandos para configuras 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#

Fuente: Propia

Se realizó la configuración en R1 acuerdo especificaciones en la tabla 16, donde se configuro la subinterfaz de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

R1(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.23, changed state to up

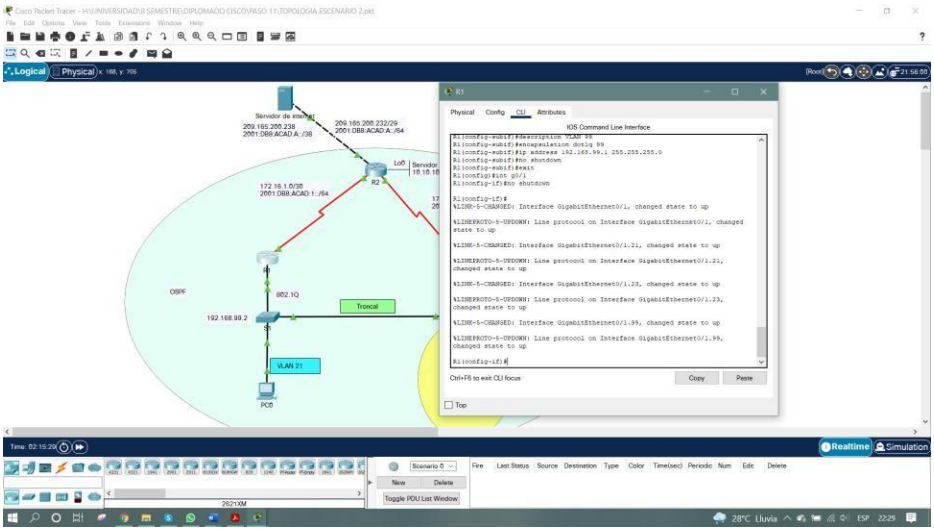
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.99, changed state to up

R1(config-if)#exit

R1(config)#

figura 18. Ejecución de los comandos para la configuración en R1



Fuente: Propia

Paso 4: Verificar la conectividad de la red

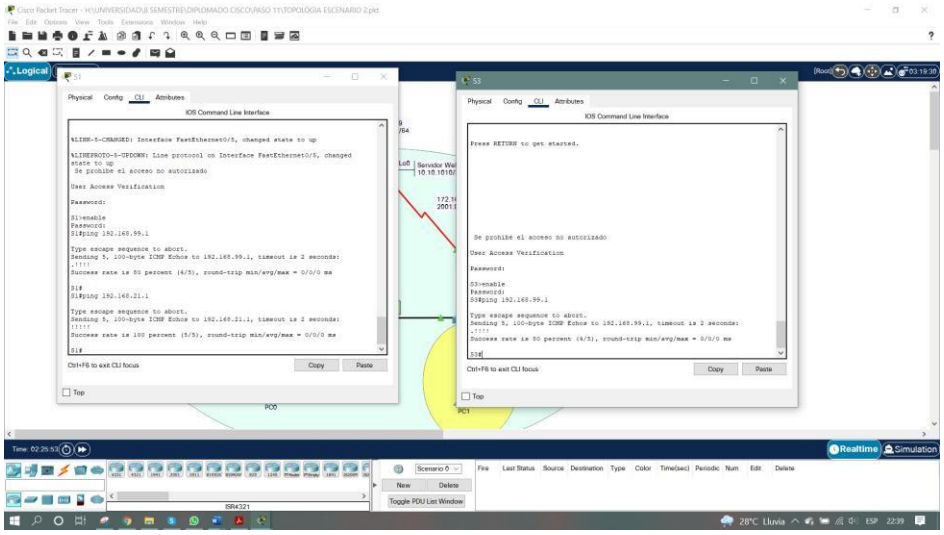
Se realizó el comando **ping** para probar la conectividad entre los dispositivos de red, verificando metódicamente la conectividad con cada dispositivo de red.

Tabla 17. Resultado de la ejecución del comando ping.

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#

Fuente: Propia

Figura 19. Resultado de la ejecución del comando ping.



Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF.

Paso 1: Configurar OSPF en el R1.

Se realiza la tabla para la configuración de OSPF, a través de protocolo de routing en R1 como se especifica en la siguiente tabla 18.

Tabla 18. Comandos para configurar OSPF en R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#config t R1(config)#**router ospf 1** R1(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#

Fuente: Propia

Se realizó la configuración en R1 acuerdo especificaciones en la tabla 18, donde se configuro OSPF de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

Se realiza la tabla para la configuración de OSPF, a través de protocolo de routing en R2 como se especifica en la siguiente tabla 19.

Tabla 19. Comandos para configurar OSPF en 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#

Fuente: Propia

Se realizó la configuración en R2 acuerdo especificaciones en la tabla 19, donde se configuro OSPF de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

R2>enable

Password:

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 R3

Se realiza la tabla para la configuración de OSPFv3, a través de protocolo de routing en R3 como se especifica en la siguiente tabla 20.

Tabla 20. Comandos para configurar OSPFv3 en R2.

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#

Fuente: Propia

Se realizó la configuración en R3 acuerdo especificaciones en la tabla 20, donde se configuro OSPFv3 de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

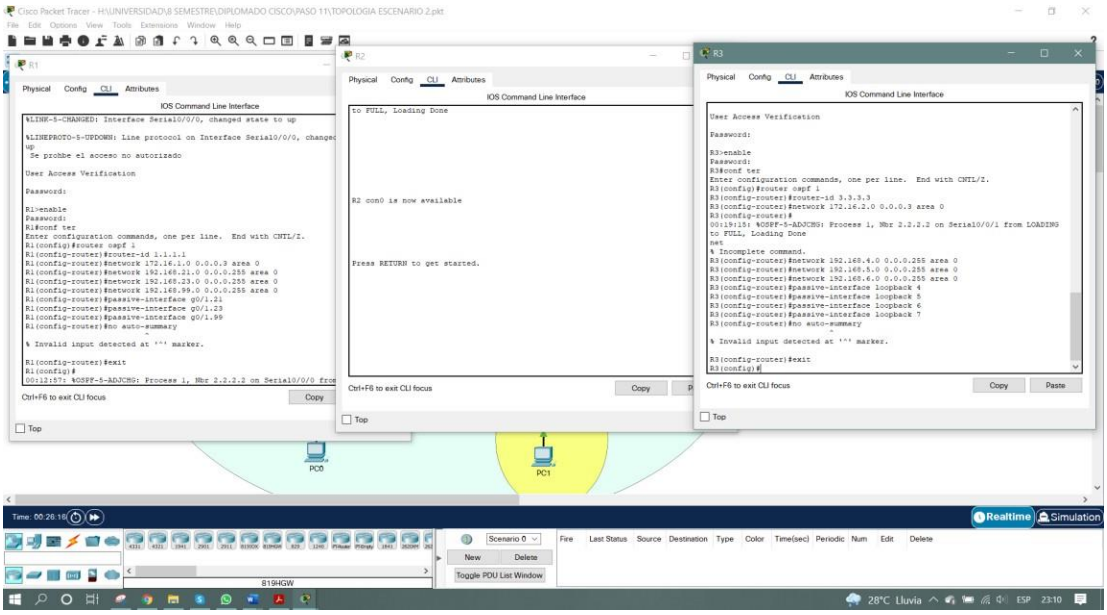
^

% Invalid input detected at '^' marker.

R3(config-router)#exit

R3(config)#

figura 20. Ejecución de los comandos para configuración de R3.



Fuente: Propia

Paso 4: Verificar la información de OSPF

Se realizó la verificación de los comandos CLI adecuado para la verificación del funcionamiento OSPF, como se muestra en la tabla 21.

Tabla 21. Comandos para verificación 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**

Fuente: Propia

Se ejecuto la verificación de los comandos de CLI donde se Verifico la configuración de OSPF, se obtuvo en cada uno de los comandos resultados exitosos como se evidencia a continuación.

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

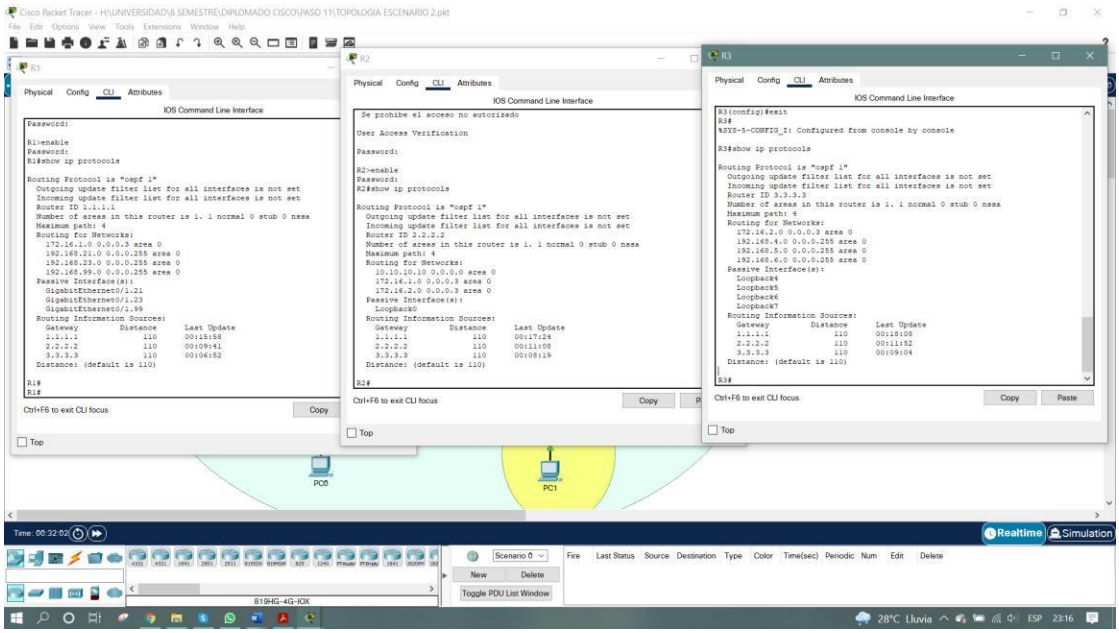
2.2.2.2 110 00:11:52

3.3.3.3 110 00:09:04

Distance: (default is 110)

R3#

figura 21. Ejecución del comando **show ip protocols**.



Fuente: Propia

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

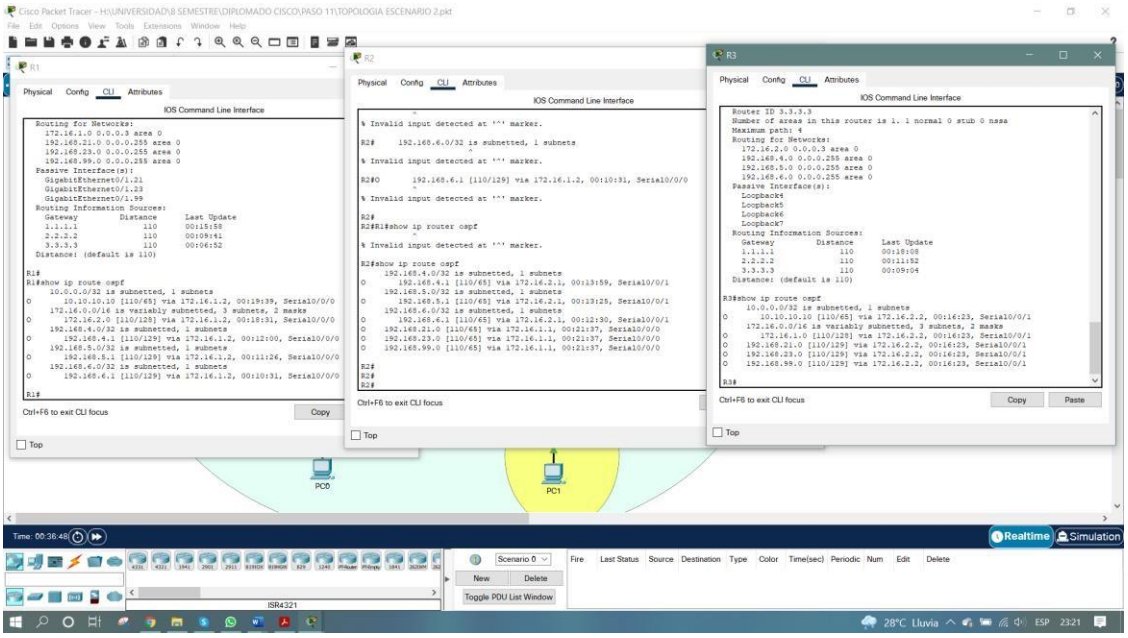
O 192.168.4.1 [110/129] via 172.16.1.2, 00:12:00, Serial0/0/0

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#

figura 22. Ejecución del comando **show ip route ospf.**



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

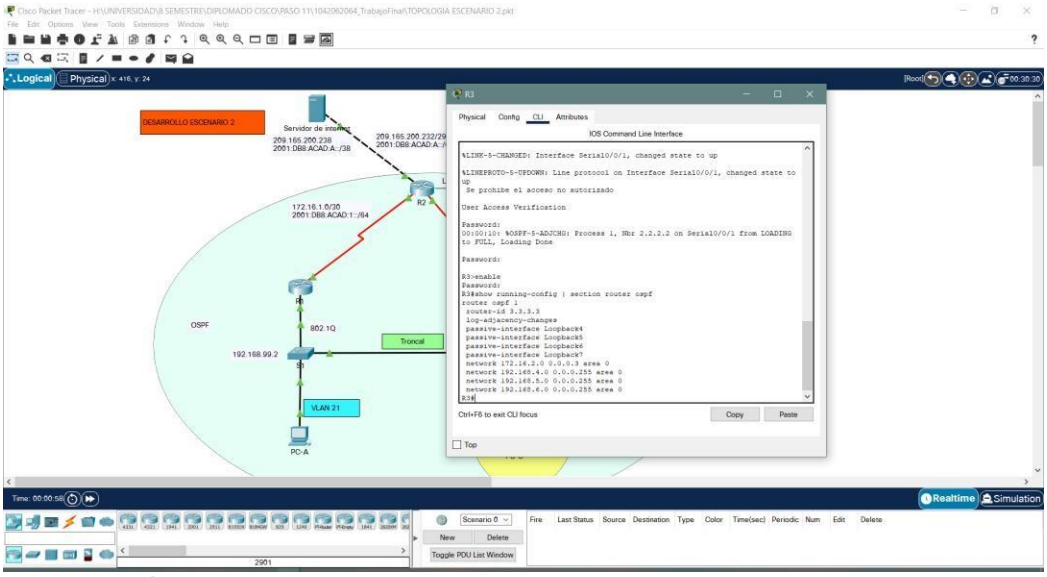
network 192.168.23.0 0.0.0.255 area 0

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#
```

figura 23. Ejecución del comando **show running-config | section router ospf.**



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

Se realizó la verificación de los comandos para la configuración DHCP en las VLAN en R1, como se muestra en la tabla 22.

Tabla 22. Configuración DHCP en R1

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#

Fuente: Propia

Se realizó la configuración en R1 acuerdo especificaciones en la tabla 22, donde se configuro DHCP en las VLAN, de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

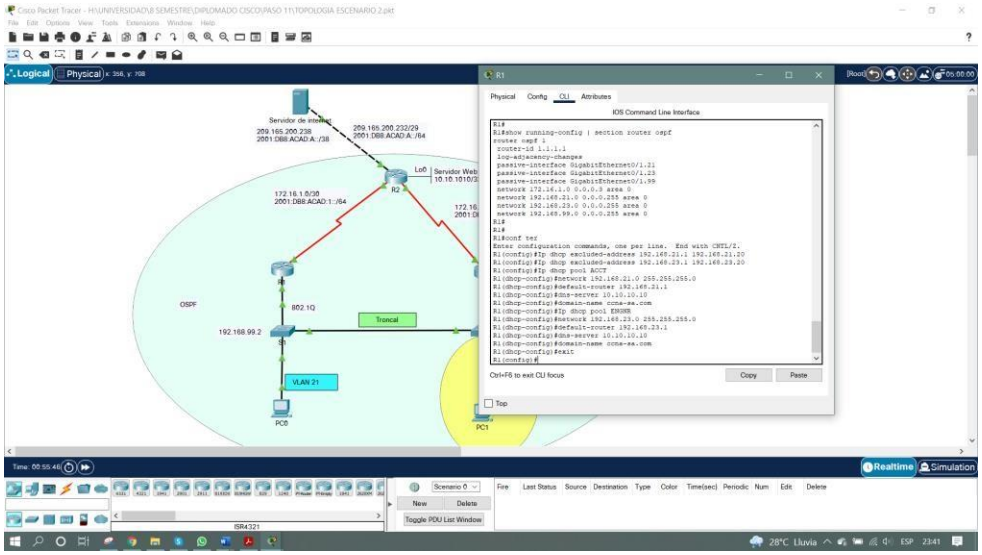
R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#domain-name ccna-sa.com

R1(dhcp-config)#exit

R1(config)#

figura 24. Ejecución de los comandos para configuración de DHCP R1.



Fuente: Propia

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

Se realizó la verificación de los comandos para la configuración NAT estática y dinámica en el R2, como se muestra en la tabla 23.

Tabla 23. Configuración 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#

Fuente: Propia

Se realizó la configuración en R2 acuerdo especificaciones en la tabla 22, donde se configuro NAT estática y dinámica, de acuerdo con el requerimiento de la topología, como se evidencia a continuación.

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

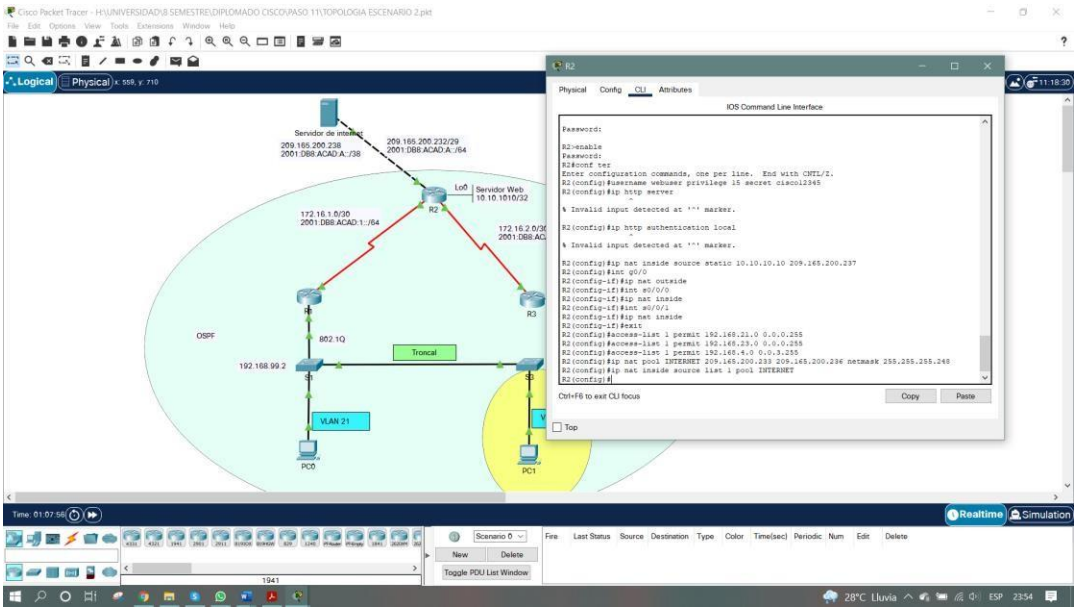
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

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)#

figura 25. Configuración de NAT estática y dinámica.



Fuente: Propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

Se realizó las respectivas verificaciones de las configuraciones de DHCP y NAT estática con el fin de evidenciar el correcto funcionamiento, se realizo los siguientes pasos como se muestra en la tabla 24.

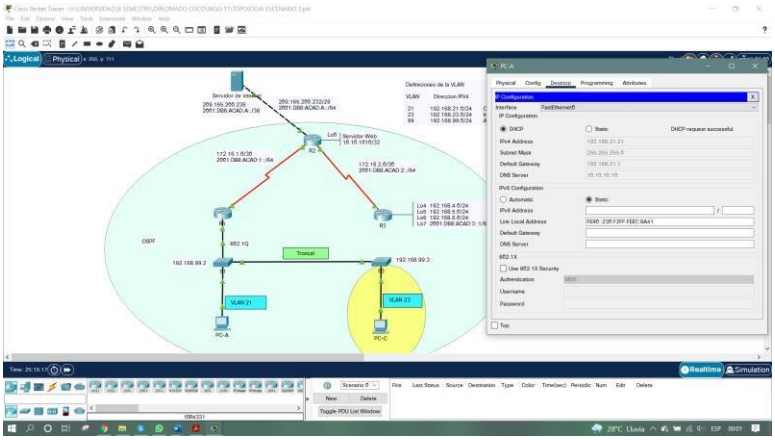
Tabla 24. Verificación de las configuraciones DHCP y NAT.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Ip address 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Ip address 192.168.23.21
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 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

Fuente: Propia

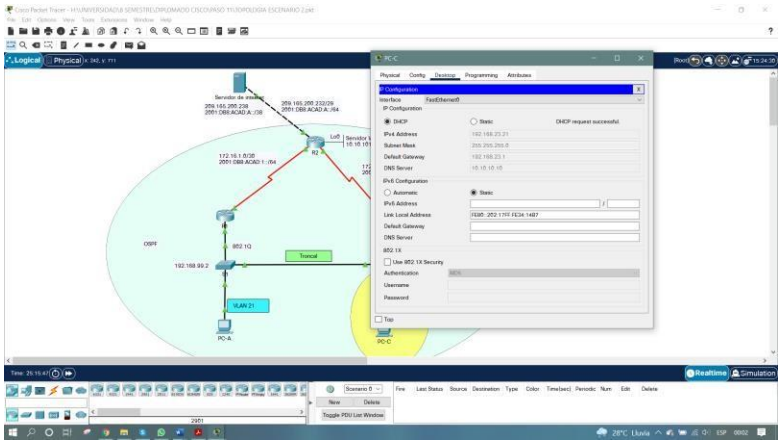
Se ejecuto la verificación de las configuraciones de DHCP y NAT estática, donde se obtuvo en cada uno de los comandos resultados exitosos como se evidencia a continuación.

figura 26. Resultados de la configuración DHCP en la PC-A.



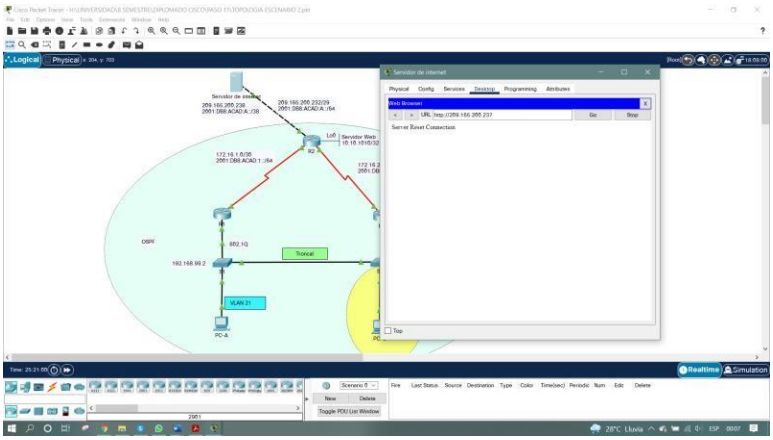
Fuente: Propia

figura 27. Resultados de la configuración DHCP en la PC-C.



Fuente: Propia

figura 28. Resultados de la configuración servicio web.



Fuente: Propia

Parte 6: Configurar NTP

Se realizó la verificación de los comandos para la configuración NTP en el R2 y R1, como se muestra en la tabla 25.

Tabla 25. Configuración de NTP en R1 y R2.

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**

Fuente: Propia

Se realizó la configuración en R2 y R1, acuerdo especificaciones en la tabla 25, donde se configuro NAT, acuerdo el requerimiento de la topología, como se evidencia a continuación.

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#

%SYS-5-CONFIG_I: Configured from console by console

R1#

Verifique la configuración de NTP en R1.

R1#show ntp associations

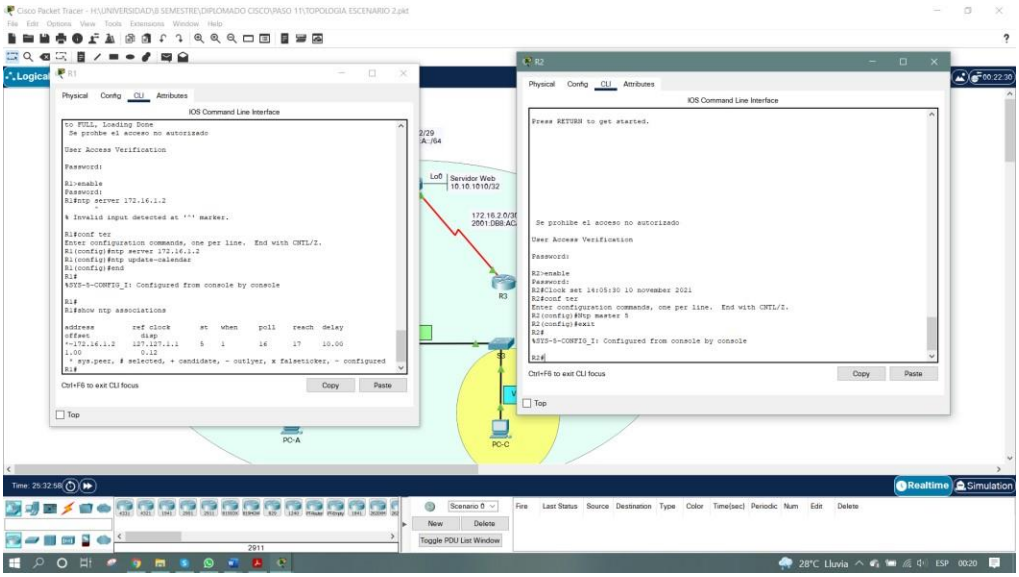
address ref clock st when poll reach delay offset disp

*~172.16.1.2 127.127.1.1 5 1 16 17 10.00 1.00 0.12

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#

figura 29. Configuración y ejecución de los comandos en R2 y 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

Se realizó la verificación de los comandos para la configuración Restricción del acceso a las líneas VTY en el R2, como se muestra en la tabla 26.

Tabla 26. Restricción de acceso líneas VTY.

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

Fuente: Propia

Se realizó la configuración en R2, acuerdo especificaciones en la tabla 26, donde se configuro la Restricción del acceso a las líneas VTY en el R2, acuerdo el requerimiento de la topología, como se evidencia a continuación.

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

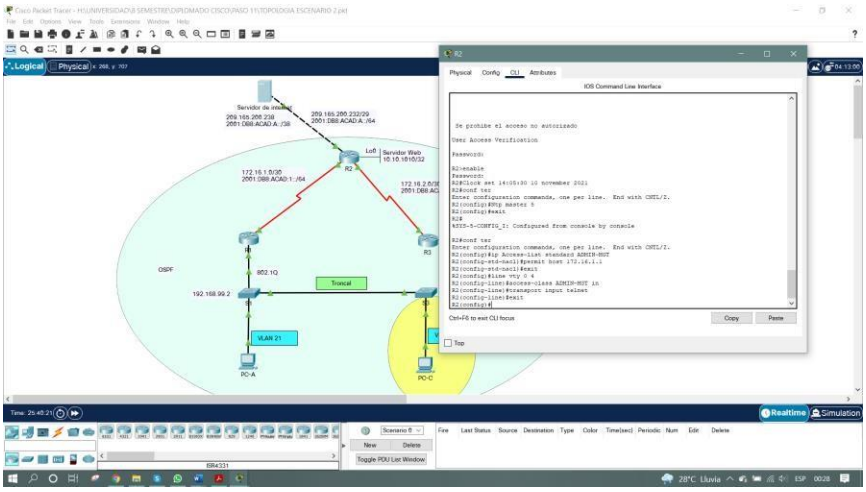
R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#transport input telnet

R2(config-line)#exit

R2(config)#

figura 30. Configuración de restricción de acceso líneas VTY en R2.



Fuente: Propia

Se realiza la comprobación de la configuración desde R1, obteniendo el siguiente resultado.

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

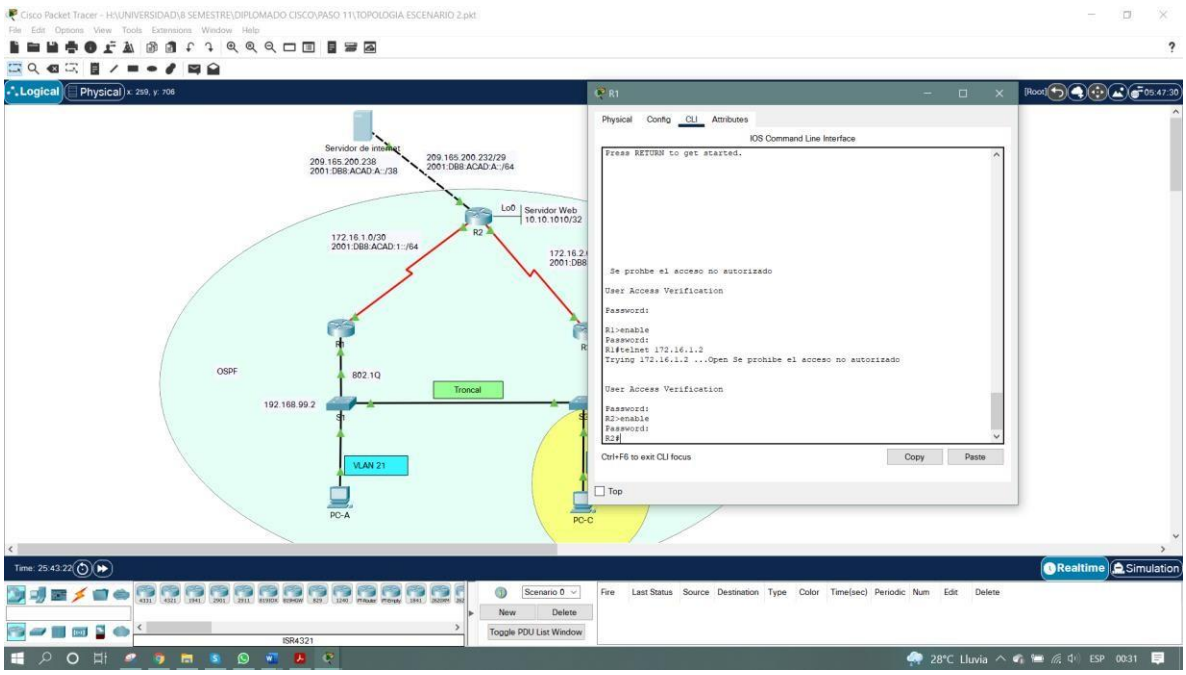
Password:

R2>enable

Password:

R2#

figura 31. Verificación de la configuración Telnet desde R1.



Fuente: Propia

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

Se realizó la verificación de los comandos CLI adecuado para la verificación del funcionamiento de la red, como se muestra en la tabla 27.

Tabla 27. Comandos para verificación de las configuraciones.

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**

Fuente: Propia

Se ejecuto la verificación de los comandos de CLI donde se Verifico la configuración de la red, se obtuvo en cada uno de los comandos resultados exitosos como se evidencia a continuación.

Se ejecuta el comando **show access-lists.**

```
R2#show access-lists
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#
```

Se ejecuta el comando **show ip interface.**

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
Internet address is 209.165.200.233/29
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
```

RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)
Internet address is 172.16.1.2/30
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Serial0/0/1 is up, line protocol is up (connected)
Internet address is 172.16.2.2/30

Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Loopback0 is up, line protocol is up (connected)
Internet address is 10.10.10.10/32
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1514bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent

IP fast switching is disabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP Fast switching turbo vector
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
Vlan1 is administratively down, line protocol is down
Internet protocol processing disabled
R2#

Se ejecuta el comando **show ip nat translations.**

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.237:80 10.10.10.10:80
209.165.200.238:1025209.165.200.238:1025
R2#

Verificación de los comandos ping en los PC.

PC-A

C:\>ping 209.165.200.238
Pinging 209.165.200.238 with 32 bytes of data:
Reply from 209.165.200.238: bytes=32 time=11ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=6ms TTL=126

Ping statistics for 209.165.200.238:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 12ms, Average = 10ms
C:\>

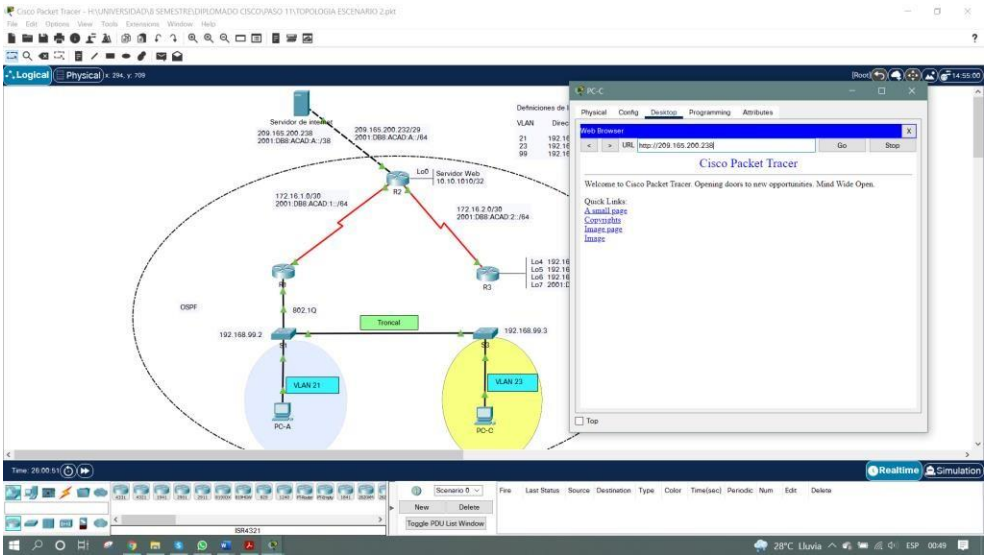
PC-C

C:\>PING 209.165.200.238
Pinging 209.165.200.238 with 32 bytes of data:
Reply from 209.165.200.238: bytes=32 time=9ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126

Ping statistics for 209.165.200.238:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 9ms, Maximum = 12ms, Average = 11ms
C:\>

Verificación de servidor web

figura 32. Ejecución del comando **http://209.165.200.238**.



Fuente: Propia

CONCLUSIONES

Es de resaltar, que el desarrollo de 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.

Se logró una satisfactoria conexión, configuración y simulación de los dispositivos de las redes en los correspondientes a los escenarios.

Finalmente se expresas satisfacción por el aprendizaje adquirido durante el desarrollo del diplomado y la aplicación de la teoría vista den la plataforma Cisco, para aplicar un correcto Subneteo y enrutamiento en una red, que la profesión Ingeniería de Sistemas requiere aplicar en todos los campos de la vida profesional real.

BIBLIOGRAFIA

CISCO. "Exploración de la red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

CISCO. " Configuración de un sistema operativo de red. Fundamentos de Networking".{En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. "Protocolos y comunicaciones de red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. " Acceso a la red. Fundamentos de Networking".{En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. "Ethernet: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. "Capa de red: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. " División de redesIP en subredes: Fundamentos de Networking.". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. "Capa de Transporte: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. "Capa de Aplicación. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. "Conceptos de Routing: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. " Routing Estático: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. " Routing Dinámico: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

UNAD "Principios de Enrutamiento [OVA]". {En línea}. {28 de noviembre de 2021} Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. " Configuración del Switch: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. "VLANs. Principios de Enrutamiento y Conmutación. {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. "Listas de control de acceso. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. " DHCP. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. " NAT para IPv4. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. " Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10