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

ERICKA MARCELA CUTA SUTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

FUSAGASUGA

2021

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

ERICKA MARCELA CUTA SUTA

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR /TUTOR

RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

FUSAGASUGA

2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Fusagasuga, Diciembre 1, 2021

DEDICATORIA

Primeramente, a Dios por permitirme completar con éxito una meta que comencé y, con el tiempo, se convirtió en una realidad.

Mi hija Angelita que es mi mayor apoyo en mi vida para seguir adelante. Mis padres, Cecilia y Humberto, que siempre me han querido incondicionalmente y me han enseñado a trabajar duro para lograr todas mis metas. Mi hermano Oscar que nunca se ha ido de mi lado y siempre ha estado conmigo. Todos mis seres queridos por ayudarme en cada momento de mis estudios y mi tutor, el profesor Raúl Bareño, que fue mi guía, apoyo para avanzar en este proceso.

Gracias.

AGRADECIMIENTO

En primer lugar, deseo expresar mi agradecimiento a Dios y al ángel enviado del cielo (Gustavo Adolfo) que siempre estuvo conmigo apoyándome y acompañándome en cada paso que daba, sus consejos fueron siempre los acertados, cuando más los necesitaba y que gracias a él hoy he logrado llegar hasta acá. Usted formó parte importante en mi vida, con sus aportes profesionales, muchas gracias por sus palabras de aliento, cuando más las necesite. Gracias a mi tutor el ingeniero Raúl Bareño, sin usted y sus virtudes, su paciencia y constancia este trabajo no lo hubiese logrado tan fácil.

A mi hija, padres y hermano, quienes han sido siempre el motor que impulsa mis sueños y esperanzas, quienes estuvieron siempre a mi lado en los días y noches más difíciles durante mis horas de estudio. Siempre han sido mis mejores guías de vida. Gracias por ser quienes son y por creer en mí.

A mis compañeros, mis amigos y compañeros de viaje, que hoy culminamos esta aventura. Hoy cerramos un capítulo maravilloso en esta historia de vida y no puedo dejar de agradecerles por su apoyo y constancia.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El presente trabajo es realizado con el objetivo de poner en práctica los conocimientos adquiridos en el Diplomado De Profundización CISCO (Diseño e Implementación de soluciones integradas LAN/WAN). Se trabajo sobre el manejo de redes, aplicando estos conocimientos en dos escenarios, en la cual en cada uno se debe construir su topología.

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

Respecto al escenario 2, se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Finalmente se hizo una evaluación, para probar y registrar la red mediante los comandos comunes de CLI.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes,

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 this first scenario, the devices of a small network were configured, then a router, a switch and equipment had to be configured, in addition to design the IPv4 addressing scheme for the proposed LANs. Finally, the router and switch must also be managed securely.

Regarding scenario 2, you must configure a small network to support IPv4 and IPv6 connectivity, switch security, routing between VLANs, OSPF Dynamic Routing Protocol, Dynamic Host Configuration Protocol (DHCP), Dynamic and Static Network Address (NAT) Translation, Access Control Lists (ACLs), and Server/Client Network Time Protocol (NTP). Finally, an evaluation was made, to test and register the network using the common CLI commands.

Keywords: CISCO, CCNA, Switching, Routing, Networks

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 interfaz 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.

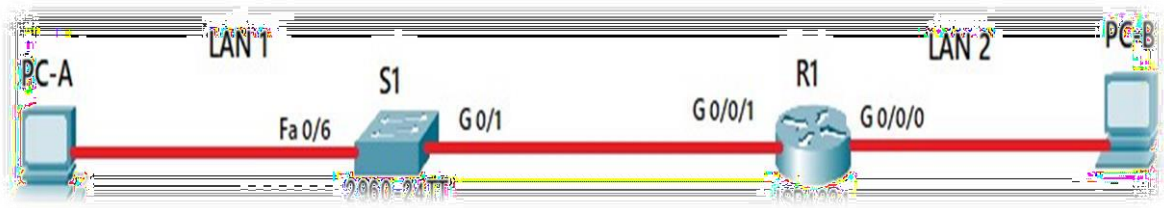
Se configurarán los dispositivos en cada uno de los escenarios y al final se verificarán si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

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.

DESARROLLO DE LOS ESCENARIOS

1. Escenario 1

figura 1. Topología escenario 1

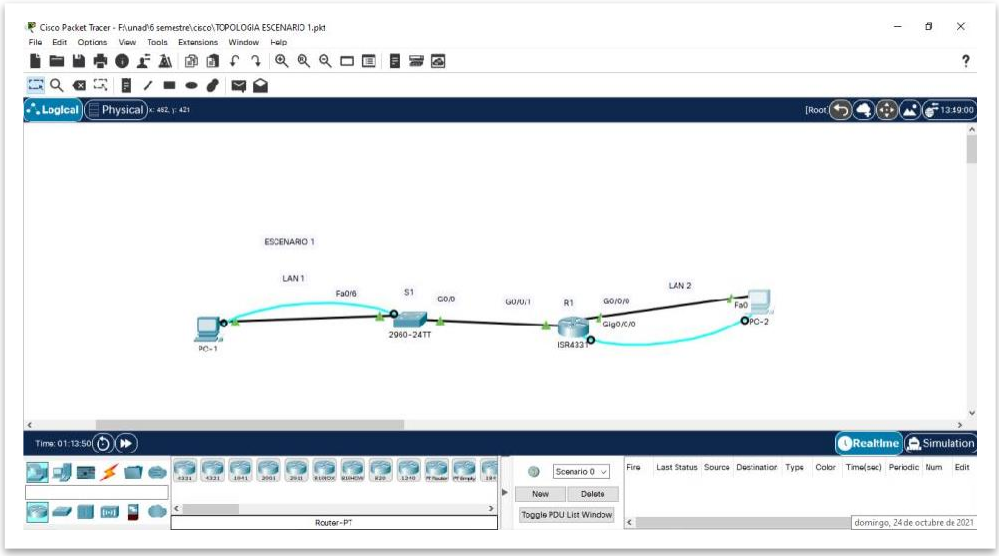


Fuente: Prueba de habilidades

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: Autor

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>
</table>

S1 SVI	Segunda dirección de host de la subred LAN1 192.168.64.2/25
PC-A	Última dirección de host de la subred LAN1 192.168.64.126/25
PC-B	Última dirección de host de la subred LAN2 192.168.64.190/26

Fuente: Autor

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: Autor

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 Inicio al modo privilegiado

Router#conf ter Ingreso a modo de configuración

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

Router(config)#no ip domain-lookup Desactivo la busqueda DNS

Router(config)#hostname R1 Asigno el nombre R1 al Router

R1(config)#ip domain-name ccna-lab.com Asigno el nombre de dominio

R1(config)#enable secret ciscoenpass Asigno contraseña modo privilegiado

R1(config)#line console 0 Ingreso a la línea consola

R1(config-line)#password ciscoconpass Asigno contraseña al acceso de consola

R1(config-line)#login Habilito la contraseña

R1(config-line)#exit Salida de la línea de consola

R1(config)#security passwords min-length 10 Establezco contraseña de long 10

R1(config)#username admin password admin1pass Creo usuario adm base local

R1(config)#line vty 0 15 Configure inicio de sesión en líneas VTY

R1(config-line)#login local Habilita la verificación de contraseña en el momento de la conexión.

R1(config-line)#exit cerrar router

R1(config)#line vty 0 15 Configure inicio de sesión en líneas VTY

R1(config-line)#transport input ssh configuración line vty para permitir sólo SSH.

R1(config-line)#login local Habilita la verificación de contraseña en el momento de la conexión.

R1(config-line)#exit salir del router

R1(config)#service password-encryption Habilita la función de cifrado de la contraseña

R1(config)#banner motd "CCNA-Acceso restringido" configuracion de un mensaje de inicio de sesión.

R1(config)#int g0/0/0 configuración de la interfaz y subinterfaces.

R1(config-if)#description Vlan2 Bikes Suministrar una descripcion

R1(config-if)#ip address 192.168.64.129 255.255.255.192 Asigna una direccion

R1(config-if)#no shutdown Reinicia una interfaz desactivada

R1(config-if)#exit cerrar session

R1(config)#int g0/0/1 configuración de la interfaz y subinterfaces.

R1(config-if)#description Vlan2 Bikes Suministrar una descripcion

R1(config-if)#ip address 192.168.64.1 255.255.255.128 Asigna una Direccion

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 Cierra sesión

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 Cierra sesión

R1#

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

R1#

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: Autor

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 Ingresa al modo Privilegiado

Switch#conf terminal Ingreso a modo de configuración

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

Switch(config)#no ip domain-lookup habilita la conversion de nombre a dirección de router

Switch(config)#hostname S1 Asigno el nombre S1 al router

S1(config)#ip domain-name ccna-lab.com asigno nombre de dominio

S1(config)#enable secret ciscoenpass Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio

S1(config)#line console 0 ingreso a la linea de consola

S1(config-line)#password ciscoconpass Asigno contraseña al acceso de consola

S1(config-line)#login Habilito la contraseña

S1(config-line)#exit cerrar session

S1(config)#username admin password admin1pass Creo usuario adm base loca

S1(config)#line vty 0 15 Configure inicio de sesión en líneas VTY

S1(config-line)#login local Habilita la verificación de contraseña en el momento de la conexión.

S1(config-line)#exit Cierra sesión

S1(config)#line vty 0 15 Configure inicio de sesión en líneas VTY

S1(config-line)#transport input ssh configuración line vty para permitir sólo SSH.

S1(config-line)#login local Habilita la verificación de contraseña en el momento de la conexión.

S1(config-line)#exit cierra sesión

S1(config)#service password-encryption Habilita la función de cifrado de la contraseña

S1(config)#banner motd "CCNA-Acceso restringido" configuracion de un mensaje de inicio de sesión.

S1(config)#crypto key generate rsa comando del modo de configuración global

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 Configurar un gateway predeterminado en un switch

S1(config)#do wr configurar el router o switch

Building configuration...

[OK]

S1(config)#exit cerrar sesion

S1#

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

S1#

Paso 2. Configurar los equipos

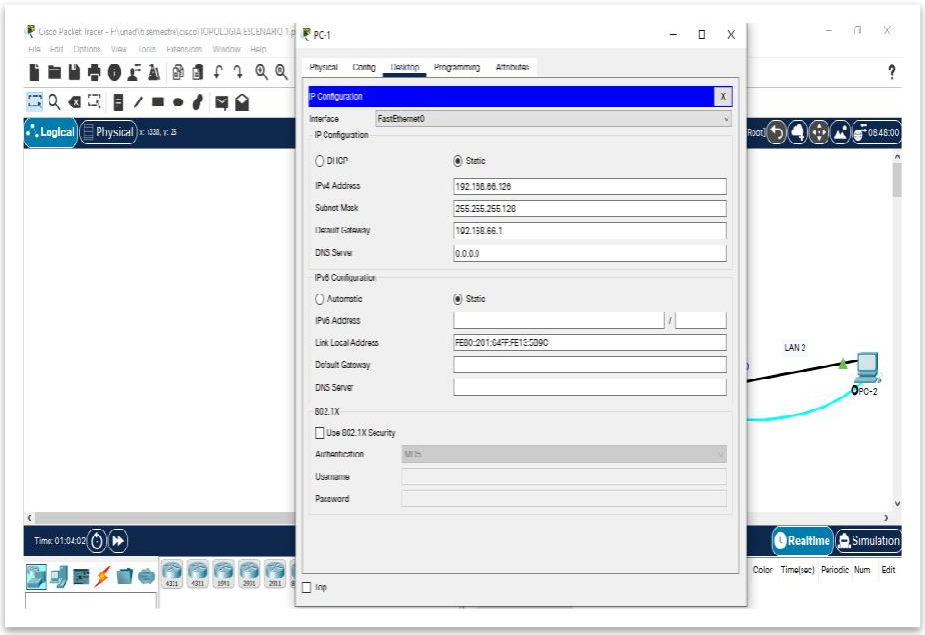
Se realizó la Configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, así mismo se la configuración de red del host con el comando ipconfig /all

Tabla 4 Configuración de los equipos host PC-A.

PC-A Network Configuration	
Descripción	PC-1
Dirección física	
Dirección IP	192.168.64.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.64.1

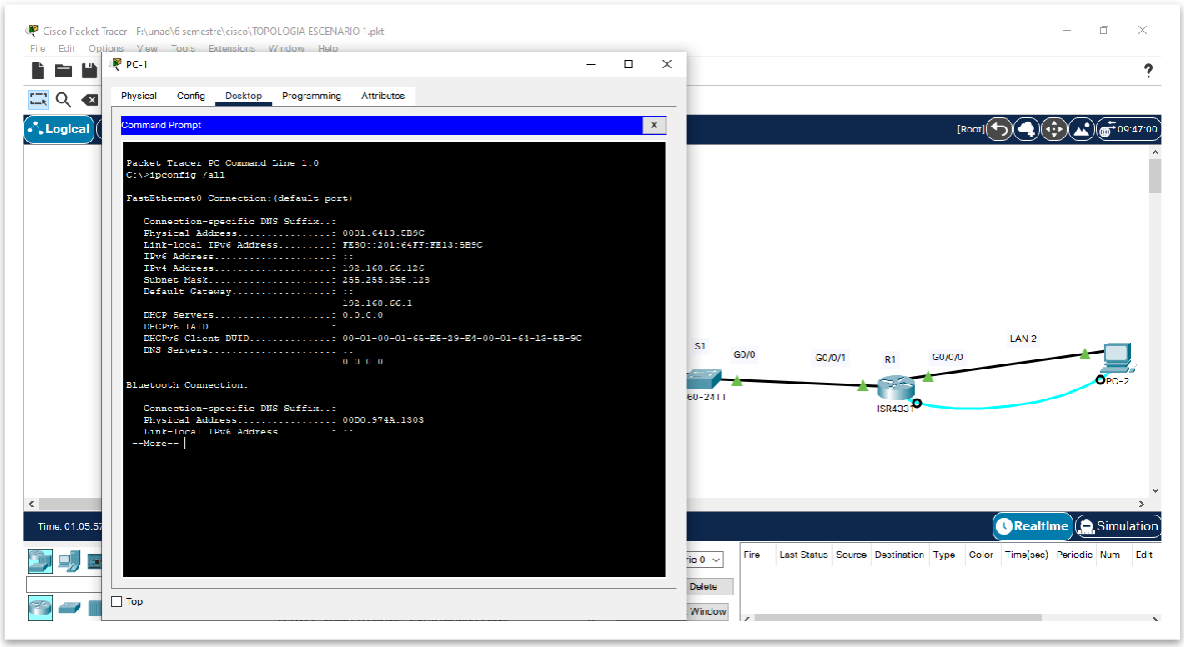
Fuente: Autor

figura 3 configuración PC-A



Fuente: Autor

figura 4 verificación comando ipconfig /all en la PC-A



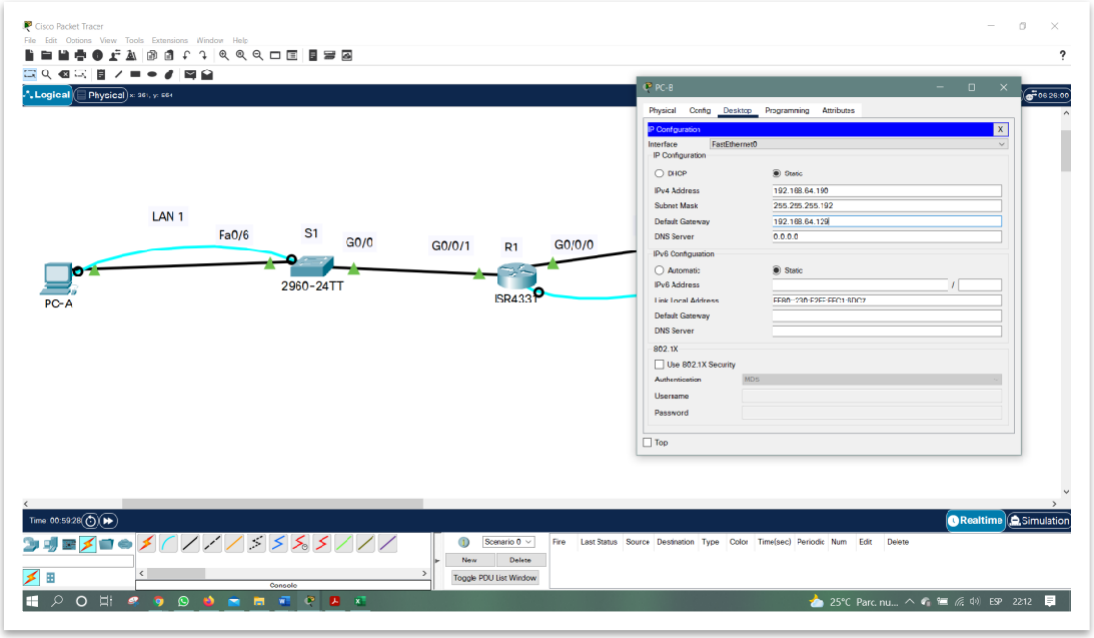
Fuente: Autor

Tabla 5 Configuración de los equipos host PC-2.

PC-2 Network Configuration	
Descripción	**PC-2**
Dirección física	
Dirección IP	192.168.64.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.64.129

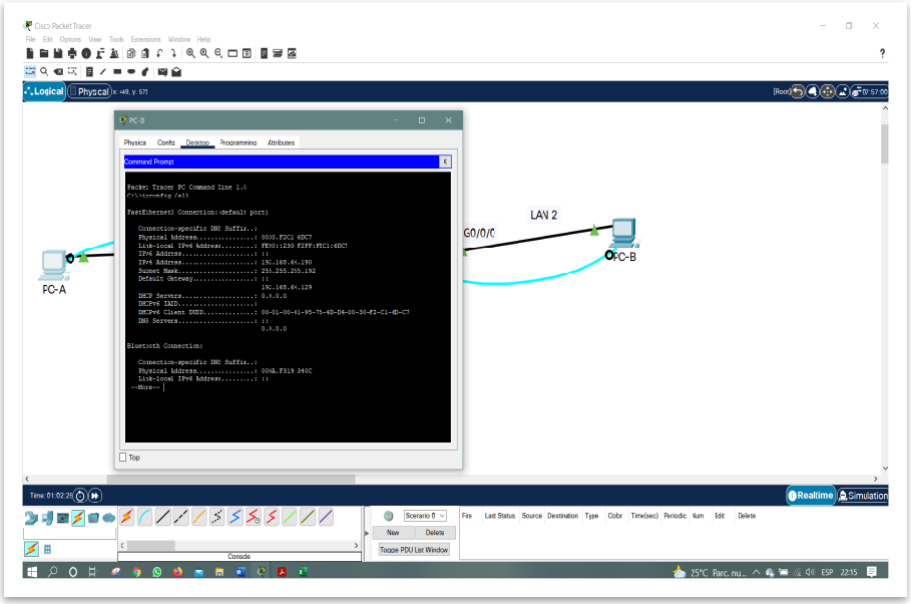
Fuente: Autor

figura 5 configuración PC-2



Fuente: Autor

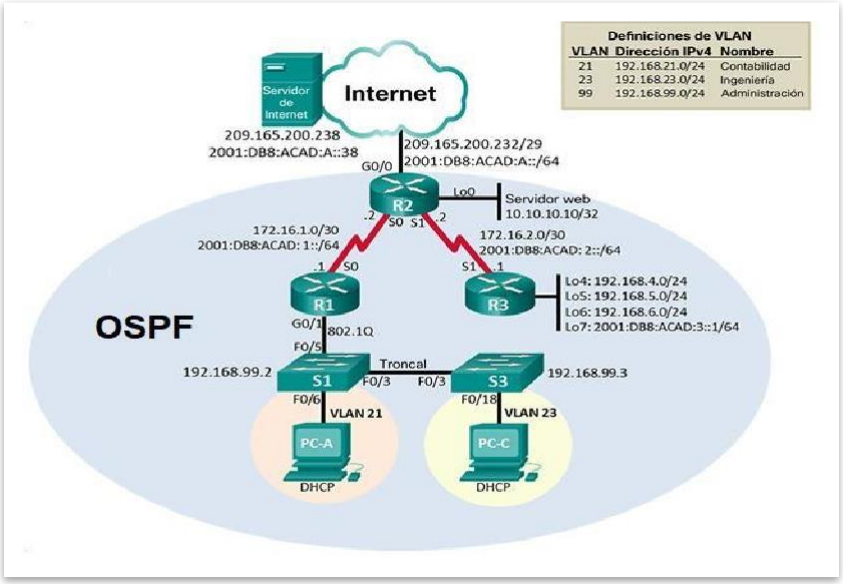
figura 6 verificación comando **ipconfig /all** en la PC-2



Fuente: Autor

2. Escenario 2

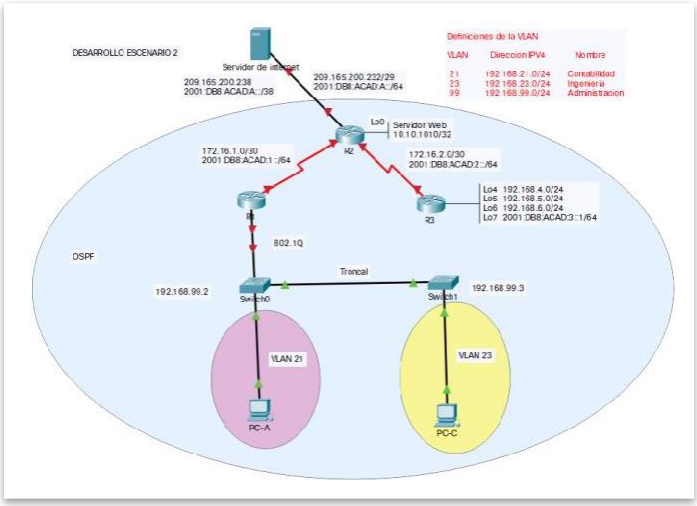
figura 7. Topología escenario 2



Fuente: Prueba de habilidades

Parte 1: Inicializar dispositivos

figura 8. Construcción de la red simulador Packet Tracer



Fuente: Autor

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

Se eliminó cada una de las configuraciones de inicio y nuevamente se vuelven a cargar los dispositivos.

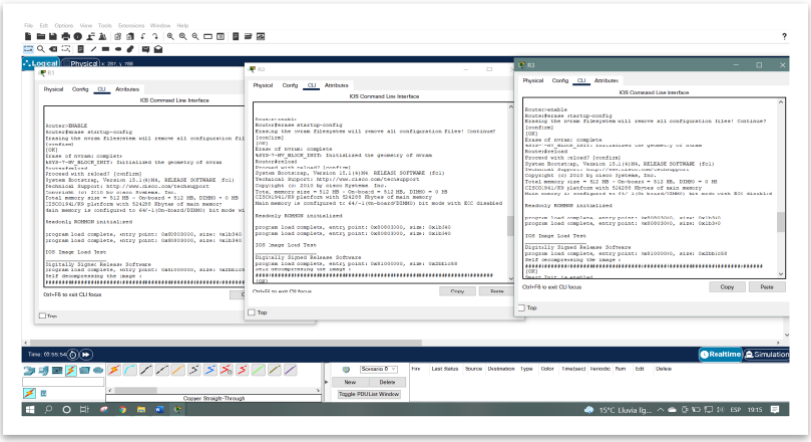
Tabla 6. Pasos para iniciar y cargar los routers y switches

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: Autor

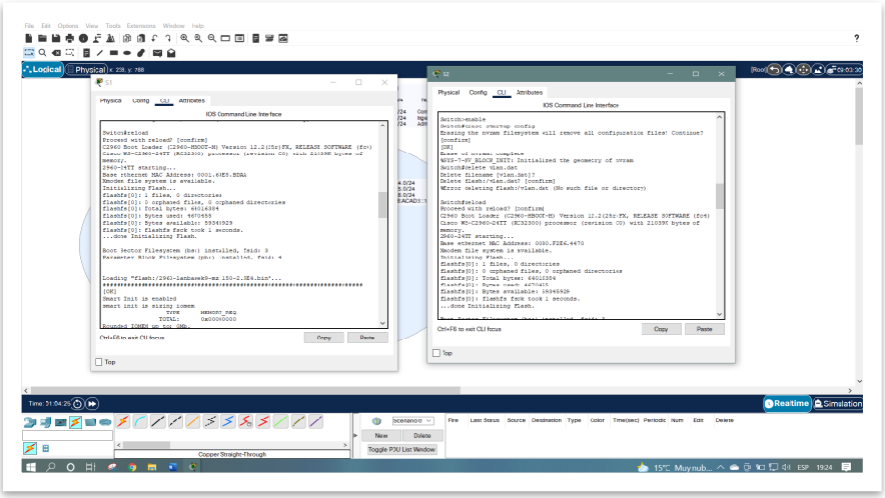
Se hizo la eliminación y cargue de cada uno de los dispositivos, teniendo en cuenta los comandos de IOS de la tabla 6, el cual podrán observar.

figura 9. Configuraciones de inicio y cargar de los Router.



Fuente: Autor

figura 3. Configuraciones de inicio y cargar de los Switches.



Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Se realiza la comprobación de redes del computador del servidor de internet, para tener el resultado que podemos ver en la tabla 7.

Tabla 7. Direcciones IP acuerdo la topología.

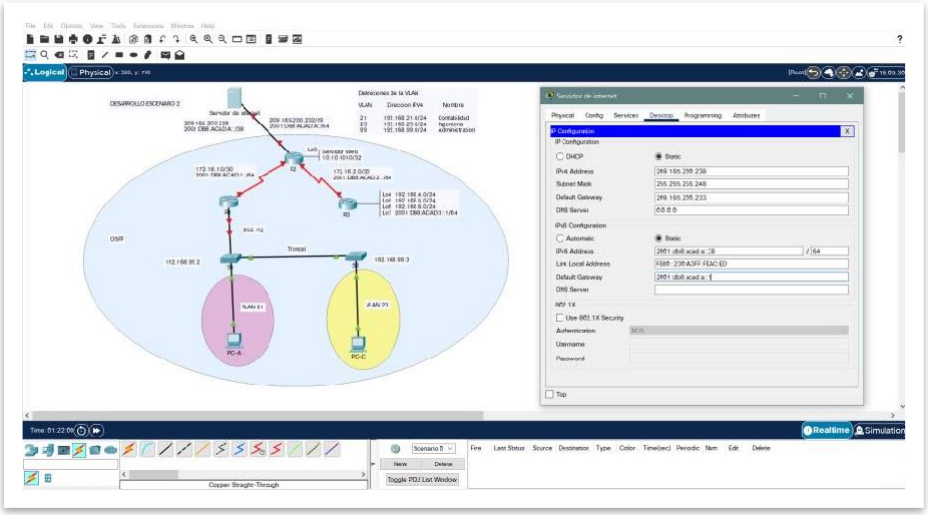
Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autor

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 realiza la configuración del computador del servidor de internet, el cual podemos ver en la figura 13..

figura 4. Configuración de la computadora servidor.



Fuente: Autor

Paso 2: Configurar R1

Fue elaborada una tabla usando los comandos utilizados en la configuración el R1, el cual podemos ver 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: Autor

Nota: Todavía no configure G0/1.

Se configuro el R1 teniendo en cuenta la tabla 8, en este paso se hizo la configuración de la seguridad de acceso, la configuración de las interfaces y la ruta predeterminada, y que podemos ver abajo.

Router>enable Inicio al modo privilegiado

Router#config term Ingreso a modo de configuracion

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

Router(config)#no ip domain-lookup Desactiva la busqueda DNS

Router(config)#hostname R1 Asigna del nombre R1 al Router

R1(config)#enable secret class Establecer la contraseña cifrada (secreta) para el modo privilegiado como “class”

R1(config)#line console 0 Ingreso a la línea consola

R1(config-line)#password cisco Establecer la contraseña de texto del modo Usuario

R1(config-line)#login Habilita la contraseña

R1(config-line)#line vty 0 4 Configura inicio de sesión en líneas VTY

R1(config-line)#password cisco Establecer la contraseña

R1(config-line)#login Habilita la contraseña

R1(config-line)#service password-encryption Habilita la función de cifrado de la contraseña

R1(config)#banner motd # Se prohibe el acceso no autorizado# Configuración de un mensaje de inicio de sesión.

R1(config)#int s0/0/0 Configuración de la interfaz y subinterfaces

R1(config-if)#description connection to R2 suministra la conexión a R2

R1(config-if)#ip address 172.16.1.1 255.255.255.252 Asigna una dirección y una máscara de subred e inicia el procesamiento IP en una interfaz

R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 configurar la dirección IPv6 unicast global en la interfaz

R1(config-if)#clock rate 128000 Tasa de transmission

This command applies only to DCE interfaces

R1(config-if)#no shutdown Reinicia una interfaz desactivada

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

R1(config-if)#exit Cierra session

R1(config)#ipv6 route ::/0 s0/0/0 Muestra el contenido de la tabla de enrutamiento IPv6

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Muestra el contenido de la tabla de enrutamiento IP

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

R1(config)#

Paso 3: Configurar R2

Se elaboro una tabla con los comandos utilizados en la configuración el R2 y que se muestra en la siguiente tabla.

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: Autor

Se configuro el R2 teniendo en cuenta la tabla 9, en este paso se hizo la configuración de la seguridad de acceso, la configuración de las interfaces y la ruta predeterminada, y que podemos ver abajo.

Router>enable Inicio al modo privilegiado

Router#config term Ingreso a modo de configuracion

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

Router(config)#no ip domain-lookup Desactivar la busqueda DNS

Router(config)#hostname R2 Asignar el nombre R2 al Router

R2(config)#enable secret class Establecer la contraseña cifrada (secreta) para el modo privilegiado como “class”

R2(config)#line console 0 Ingreso a la línea consola

R2(config-line)#password cisco Asigno contraseña a la consola

R2(config-line)#login Habilito la contraseña

R2(config-line)#line vty 0 4 Configure inicio de session en lineas VTY

R2(config-line)#password cisco Asigno contraseña a la consola

R2(config-line)#login Habilita la contraseña

R2(config-line)#service password-encryption Habilita la function de cifrado de la contraseña.

R2(config)#ip http server Especifica el método de autenticación que se utilizará para el inicio de sesión

^

% Invalid input detected at '^' marker.

R2(config)#banner motd # Se prohibe el acceso no autorizado # configurar un MOTD en el modo de configuración global

R2(config)#int s0/0/0 configuración de interfaces serial 0

R2(config-if)#description connection to R1 descripcion de la conexion a R1

R2(config-if)#ip address 172.16.1.2 255.255.255.252 Asigna una direccion

R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 configurar la dirección IPv6 unicast global en la interfaz

R2(config-if)#no shutdown Reinicia una interfaz desactivada

R2(config-if)#exit cerra sesion

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 configuración de interfaces serial 1

R2(config-if)#description connection to R3 descripcion de la conexion a R3

R2(config-if)#ip address 172.16.2.2 255.255.255.252 Asigna una direccion Ip

R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 configurar la dirección IPv6 unicast global en la interfaz

R2(config-if)#clock rate 128000 tasa de transmission

R2(config-if)#no shutdown Reinicia un interfaz desactivada

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

R2(config-if)#exit cerrar sesion

R2(config)#int g0/0 configuracion de la interfaz y subinterfaces

R2(config-if)#description connection to Internet descripcion de la conexion a internet

R2(config-if)#ip address 209.165.200.233 255.255.255.248 Asigna una direccion ip

R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 configura la direccion IPv6 unicast global en la interfaz

R2(config-if)#no shutdown Reinicia una interfaz desactivada

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 cerrar sesion

R2(config)#int loopback 0

R2(config-if)#description Simulated Web Server suministrar la descripcion del servidor web

R2(config-if)#ip address 10.10.10.10 255.255.255.255 Asigna la direccion Ip

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 Cerra sesion

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 0 Muestra el contenido de la tabla de enrutamiento IP

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

R2(config)#ipv6 route ::/0 g0/0 0 Muestra el contenido de la tabla de enrutamiento IPv6

R2(config)#

Paso 4: Configurar R3

Se elaboro una tabla con los comandos utilizados en la configuración el R3 y que se muestra en la siguiente tabla.

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: Autor

Se configuro el R3 teniendo en cuenta la tabla 10, en este paso se hizo la configuración de la seguridad de acceso, la configuración de las interfaces y la ruta predeterminada, y que podemos ver abajo.

Router>enable inicio al modo privilegiado

Router#config term ingreso a modo configuracion

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

Router(config)#no ip domain-lookup desactiva la busqueda DNS

Router(config)#hostname R3 Asigna el nombre R3 al Router

R3(config)#enable secret class Establecer la contraseña cifrada (secreta) para el modo privilegiado como “class”

R3(config)#line console 0 Ingreso a la línea consola

R3(config-line)#password cisco Asigno contraseña a la consola

R3(config-line)#login Habilita la contraseña

R3(config-line)#line vty 0 4 configure inicio de session en lineas VTY

R3(config-line)#password cisco Asigno contraseña al acceso de consola

R3(config-line)#login Habilito la contraseña

R3(config-line)#service password-encryption Habilito la function de cifrado de la contraseña

R3(config)#banner motd # Se prohibe el acceso no autorizado# configuro el mensaje de inicio de sesion

R3(config)#int s0/0/1 configuración de interfaces serial 0

R3(config-if)#description connection to R2 descripcion de la conexion a R1

R3(config-if)#ip address 172.16.2.1 255.255.255.252configurar direccion ip

R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 configurar direccion ipv6

R3(config-if)#no shutdown Activacion de interfaz

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 configurar direccion ip

%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 configurar direccion ip

%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 configurar direccion ip

%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 configurar direccion ipv6

%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 cerrar sesion

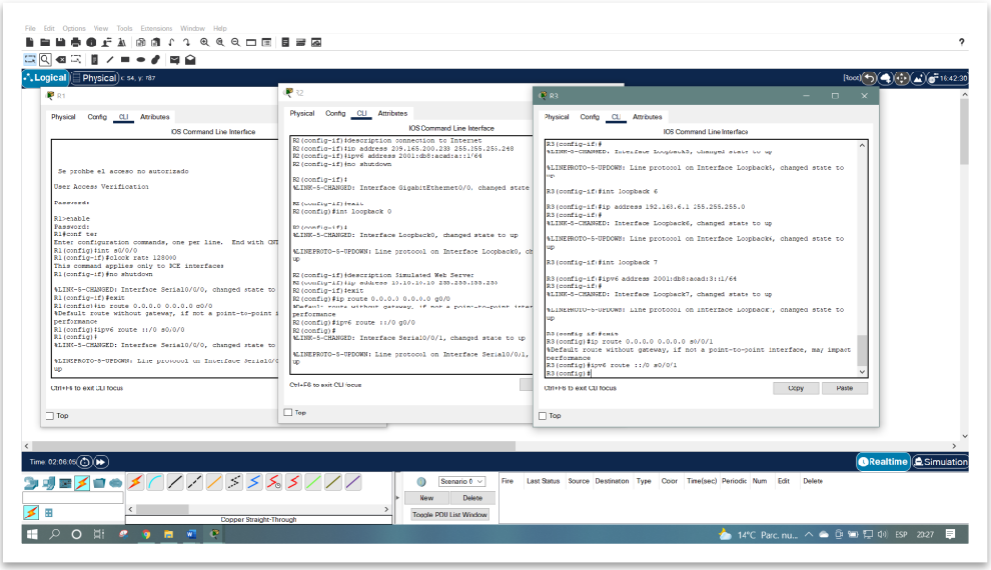
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 se configura la ruta estatica constante.

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

R3(config)#ipv6 route ::/0 s0/0/1 se configura la ruta estatica constante.

R3(config)#

figura 12. Configuración de R1, R2 y R3.



Fuente: Autor

Paso 5: Configurar S1

Se elaboro una tabla con los comandos utilizados en la configuración el S1 y que se muestra en la siguiente tabla.

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: Autor

Se configuro en S1 teniendo en cuenta la tabla 11, en este paso se hizo la configuración de la seguridad de acceso, y que podemos ver abajo.

Switch>enable inicio al modo privilegiado

Switch#config ter Ingresoa modo de configuracion

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

Switch(config)#no ip domain-lookup Desactivo la busqueda DNS

Switch(config)#hostname S1 Asigno el nombre S1 al router

S1(config)#enable secret class Especifica una capa de seguridad adicional mediante el comando enable password.

S1(config)#line console 0 Ingreso a la linea consola

S1(config-line)#password cisco contraseña de acceso

S1(config-line)#login Habilito la contraseña

S1(config-line)#line vty 0 4 Configuracion inicio de sesión en líneas VTY

S1(config-line)#password cisco Contraseña de acceso

S1(config-line)#login Habilito la contraseña

S1(config-line)#service password-encryption Habilita la function de cifrado de la contraseña

S1(config)#banner motd # Se prohibe el acceso no autorizado # configuración de un mensaje de iniciación de sesion

S1(config)#exit cerrar sesión

S1#

Paso 6: Configurar el S3

Se elaboro una tabla con los comandos utilizados en la configuración el S3 y que se muestra en la siguiente tabla.

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: Autor

Se configuro en S3 teniendo en cuenta la tabla 12, en este paso se hizo la configuración de la seguridad de acceso, y que podemos ver abajo.

Switch>enable Inicio al modo privilegiado

Switch#config term Ingreso a modo de configuración

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

Switch(config)#no ip domain-lookup Desactivo la busqueda DNS

Switch(config)#hostname S3 Asino el nombre S3 al router

S3(config)#enable secret class Especifica una capa de seguridad adicional mediante el comando enable password.

S3(config)#line console 0 Ingreso a la linea consola

S3(config-line)#password cisco Contraseña de acceso

S3(config-line)#login Habilito la contraseña

S3(config-line)#line vty 0 4 configuracioninicio de sesion en linea

S3(config-line)#password cisco Contraseña de acceso

S3(config-line)#login Habilito la contraseña

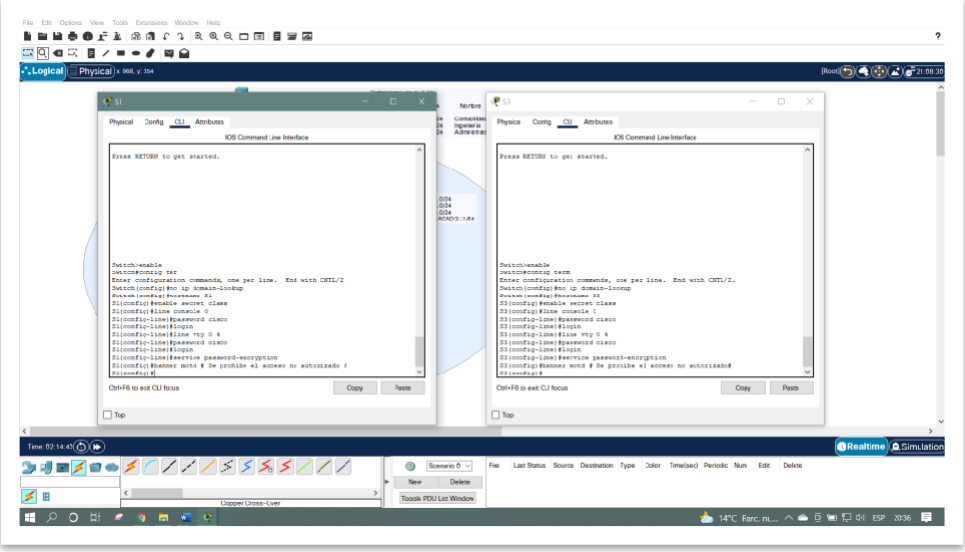
S3(config-line)#service password-encryption Habilita la function de cifrado de la contraseña

S3(config)#banner motd # Se prohibe el acceso no autorizado# configuración de un mensaje de iniciación de sesion

S3(config)#exit cerrar sesion

S3#

figura 5. Configuración de S1 y S3



Fuente: Autor

Paso 7: Verificar la conectividad de la red.

Se probó la conectividad entre los dispositivos de red usando el comando ping, y la conectividad con cada uno de los dispositivos de red fueron comprobadas.

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	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

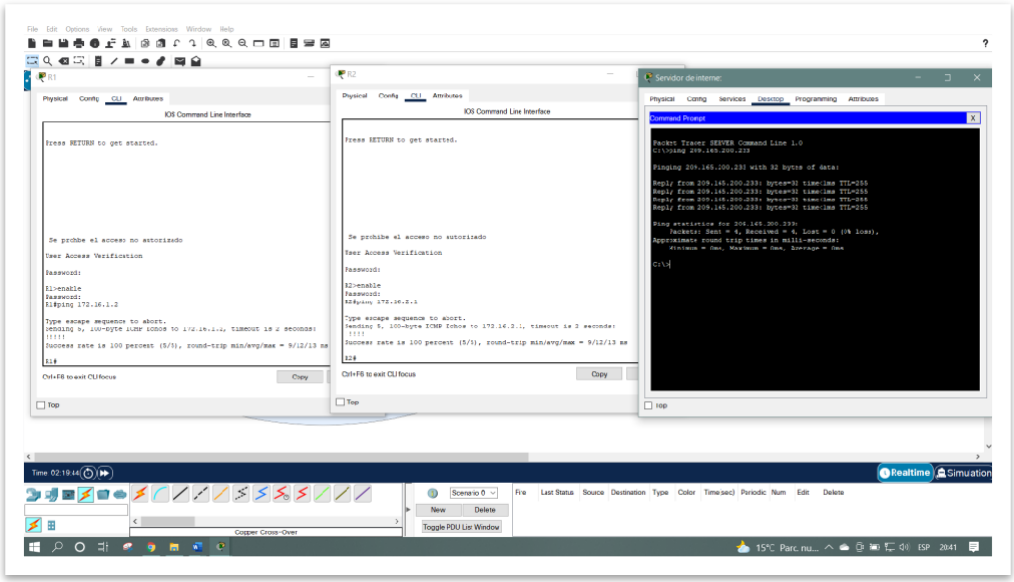
			Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 2ms C:\>

Fuente: Autor

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

Se realizó la comprobación de cada uno de los dispositivos, con el fin de confirmar que los pings utilizados fueran los adecuados en la conectividad realizada.

figura 64. Resultado de la ejecución del comando ping.



Fuente: Autor

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

Paso 1: Configurar S1

La tabla fue hecha con los comandos usando la configuración de S1 como lo podemos ver abajo.

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: Autor

Se configuro en S1 teniendo en cuenta la tabla 14, en este paso se hizo la configuración de las Vlan y la interfaz teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

S1>enable Inicio al modo privilegiado

Password: Escribir la contraseña

S1#enable Inicio al modo privilegiado

S1#conf ter Ingreso a modo de configuración

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

S1(config)#vlan 21 ingreso a config vlan 21

S1(config-vlan)#name Contabilidad se asigna el nombre a la vlan

S1(config-vlan)#vlan 23 ingreso a config vlan 23

S1(config-vlan)#name Ingenieria se asigna el nombre a la vlan

S1(config-vlan)#vlan 99 ingreso a config vlan 99

S1(config-vlan)#name Administracion se asigna el nombre a la vlan

S1(config-vlan)#exit cerrar sesión

S1(config)#int vlan 99

S1(config-if)#ip address 192.168.99.2 255.255.255.0 asigacion de direccionamiento vlan 99

S1(config-if)#

%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#no shutdown Activacion interfaz

S1(config-if)#exit cerrar sesion

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 cerrar sesion

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

La tabla se hizo con los comandos usando la configuración de S3 de acuerdo con 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: Autor

Se configuro en S3 teniendo en cuenta la tabla 15, en este paso se hizo la configuración de las Vlan y la interfaz teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

S3>enable Inicio al modo privilegiado

Password: Contraseña

S3#conf ter Ingreso a modo de configuracion

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

S3(config)#vlan 21 Ingreso configuración vlan 21

S3(config-vlan)#Name Contabilidad se asigna el nombre a la vlan

S3(config-vlan)#vlan 23 ingreso configuración vlan 23

S3(config-vlan)#name Ingenieria se asigna el nombre a la vlan

S3(config-vlan)#vlan 99 ingreso configuración vlan 99

S3(config-vlan)#name Administracion se asigna el nombre a la vlan

S3(config-vlan)#exit cerrar sesion

S3(config)#int vlan 99

S3(config-if)#ip address 192.168.99.3 255.255.255.0 configuracion direccion ip

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 Inhabilita una interfaz

%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

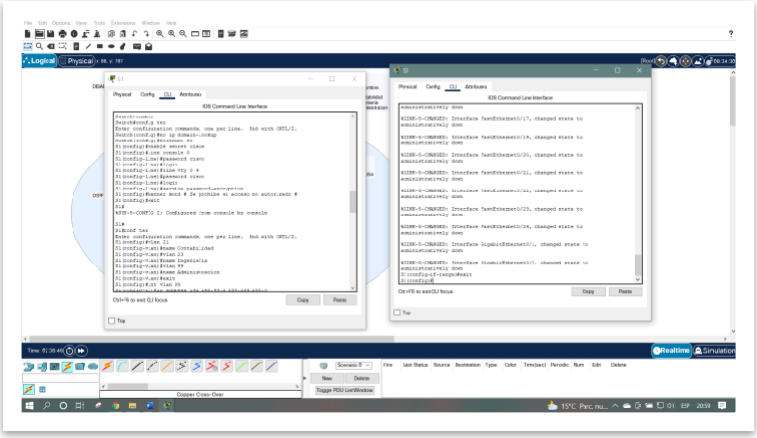
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

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

S3(config-if-range)#exit cerrar sesion

S3(config)#

figura 7. Configuración de S1 y S3



Fuente: Autor

Paso 3: Configurar R1

La tabla se hizo con los comandos usando la configuración R1 teniendo en cuenta 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: Autor

Se configuro en R1 teniendo en cuenta la tabla 16, en este paso se hizo la configuración de la subinterfaz teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R1>enable inicio al modo privilegiado

Password: contraseña

R1#conf ter ingreso a modo de configuración

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

R1(config)#int g0/1.21 configuracion de la interfaz y subinterfaz

R1(config-subif)#description VLAN 21 describir la vlan 21

R1(config-subif)#encapsulation dot1q 21

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 configurar la dirección ip

R1(config-subif)#no shutdown reiniciar una interfaz desactivada

R1(config-subif)#exit cerrar sesión

R1(config)#int g0/1.23 configuracion de la interfaz y subiterfaz

R1(config-subif)#description VLAN 23 descripcion de la vlan 23

R1(config-subif)#encapsulation dot1q 23

R1(config-subif)#ip address 192.168.23.1 255.255.255.0 configuracion direccion ip

R1(config-subif)#no shutdown reinicia una interfaz desactivada

R1(config-subif)#exit cerrar sesion

R1(config)#int g0/1.99 configuracion de la interfaz y subinterfaz

R1(config-subif)#description VLAN 99 descripcion de la vlan 99

R1(config-subif)#encapsulation dot1q 99

R1(config-subif)#ip address 192.168.99.1 255.255.255.0 configuracion direccion ip

R1(config-subif)#no shutdown reiniciar un interfaz desactivada

R1(config-subif)#exit cerrar sesión

R1(config)#int g0/1 configuracion de la interfaz y subredes

R1(config-if)#no shutdown reinicia la anterior interfaz

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

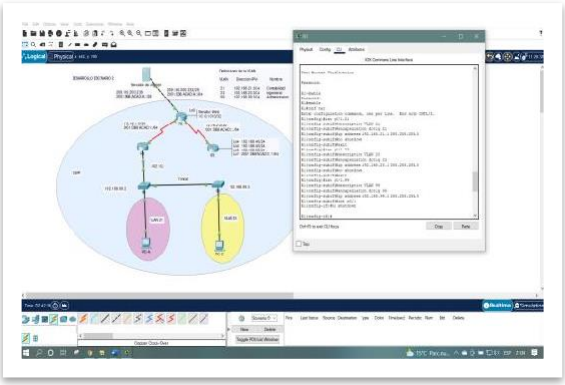
%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

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

R1(config-if)#exit cerrar sesion

R1(config)#

figura 8. Ejecución de los comandos para la configuración en R1



Fuente: Autor

Paso 4: Verificar la conectividad de la red

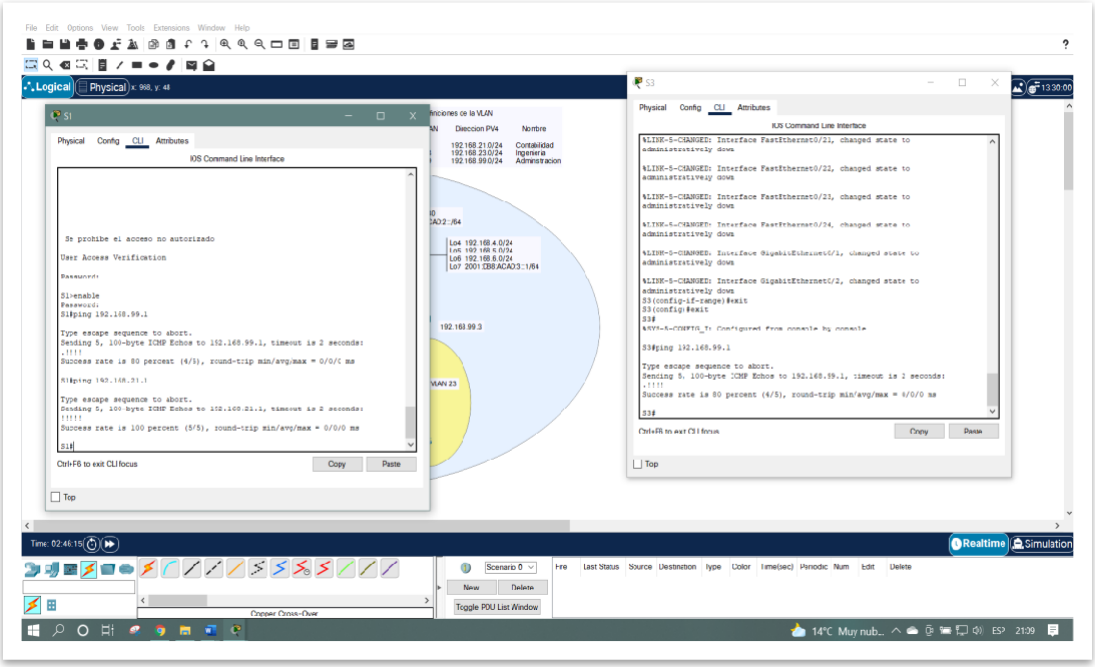
Fue probada la conectividad entre los dispositivos de red usando el comando ping igualmente se hizo la comprobación de la conectividad de los dispositivos de red.

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: Autor

Figura 9. Resultado de la ejecución del comando ping.



Fuente: Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF.

Paso 1: Configurar OSPF en el R1.

La tabla fue realizada para la configuración de OSPF, utilizando el protocolo de routing en R1, según la tabla:

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: Autor

Se configuro en R1 teniendo en cuenta la tabla 18, en este paso se hizo la configuración de OSPF, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R1>enable inicio al modo privilegiado

Password: contraseña

R1#conf ter ingreso a modo de configuracion

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

R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1 Crea una ruta “quad zero” o predeterminada

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 Añade una red a la configuración RIP

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 Añade una red a la configuración RIP

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 Añade una red a la configuración RIP

R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 Añade una red a la configuración RIP

R1(config-router)#passive-interface g0/1.21 El router no enviará información de enrutamiento por la interfaz

R1(config-router)#passive-interface g0/1.23 El router no enviará información de enrutamiento por la interfaz

R1(config-router)#passive-interface g0/1.99 El router no enviará información de enrutamiento por la interfaz

R1(config-router)#no auto-summary

^

% Invalid input detected at '^' marker.

R1(config-router)#exit

R1(config)#

Paso 2: Configurar OSPF en el R2

La tabla fue realizada para la configuración de OSPF, utilizando el protocolo de routing en R2, según la tabla:

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: Autor

Se configuro en R2 teniendo en cuenta la tabla 19, en este paso se hizo la configuración de OSPF, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R2>enable inicio al modo privilegiado

Password: contraseña

R2#conf ter ingreso a modo de configuración

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 añade una red a la configuración OSPF

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 0 añade una red a la configuración OSPF

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0

R2(config-router)#passive-interface loopback 0 0 añade una red a la configuración OSPF

R2(config-router)#no auto-summary desabilita el auto resumen

^

% Invalid input detected at '^' marker.

R2(config-router)#

Paso 3: Configurar OSPFv3 en el R3

La tabla fue realizada para la configuración de OSPFv3, utilizando el protocolo de routing en R3, según la tabla:

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: Autor

Se configuro en R3 teniendo en cuenta la tabla 20, en este paso se hizo la configuración de OSPFv3, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R3>enable inicio al modo privilegiado

Password: contraseña

R3#conf ter ingreso a modo de configuración

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 Añade una red a la configuración

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 Añade una red a la configuración

R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 Añade una red a la configuración

R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 Añade una red a la configuración

R3(config-router)#passive-interface loopback 4 El router no enviará información de enrutamiento por la interfaz

R3(config-router)#passive-interface loopback 5 El router no enviará información de enrutamiento por la interfaz

R3(config-router)#passive-interface loopback 6 El router no enviará información de enrutamiento por la interfaz

R3(config-router)#passive-interface loopback 7 El router no enviará información de enrutamiento por la interfaz

R3(config-router)#no auto-summary Desabilita el auto resumen

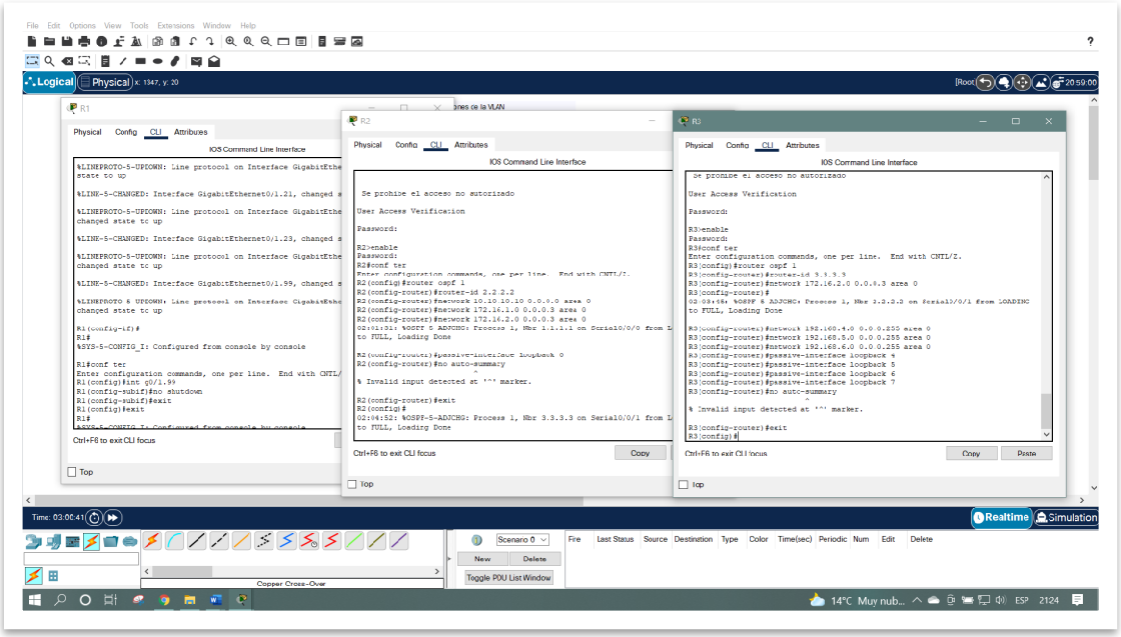
^

% Invalid input detected at '^' marker.

R3(config-router)#exit cerrar sesion

R3(config)#

figura 10. Ejecución de los comandos para configuración de R1, R2 Y R3.



Fuente: Autor

Paso 4: Verificar la información de OSPF

Se comprobaron los comandos CLI en el funcionamiento de OSPF, como podemos ver en la siguiente tabla:

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: Autor

Se comprobaron los comandos de CLI de la configuración de OSPF, y de cada uno de los comandos salieron los resultados esperados, el cual podemos ver abajo.

R1>enable inicio al modo privilegiado

Password: contraseña

R1#show ip protocols muestra el protocolo de la ip

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 Inicio al modo privilegiado

Password: contraseña

R2#show ip protocols muestra los protocolos de ip

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 muestra protocolos de ip

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

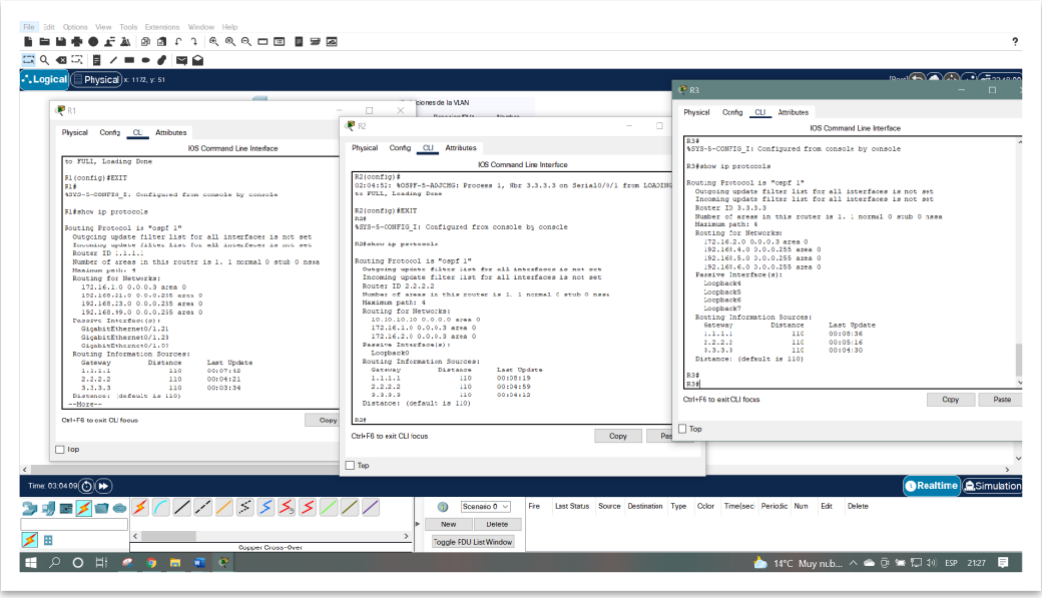
2.2.2.2 110 00:11:52

3.3.3.3 110 00:09:04

Distance: (default is 110)

R3#

figura 11. Ejecución del comando show ip protocolos.



Fuente: Autor

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

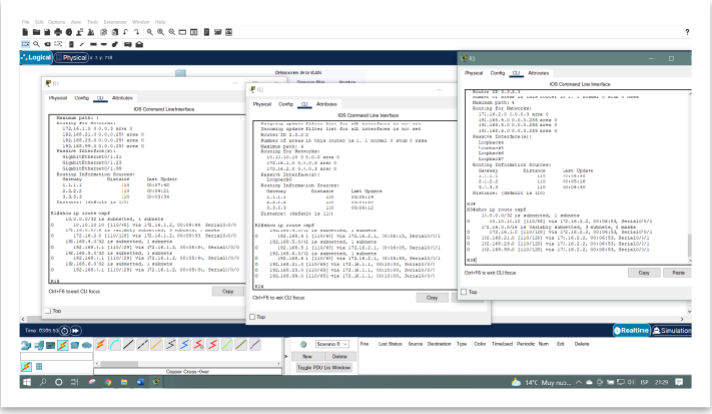
O 192.168.21.0 [110/129] via 172.16.2.2, 00:16:23, Serial0/0/1

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 12. Ejecución del comando show ip route ospf.



Fuente: Autor

```
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

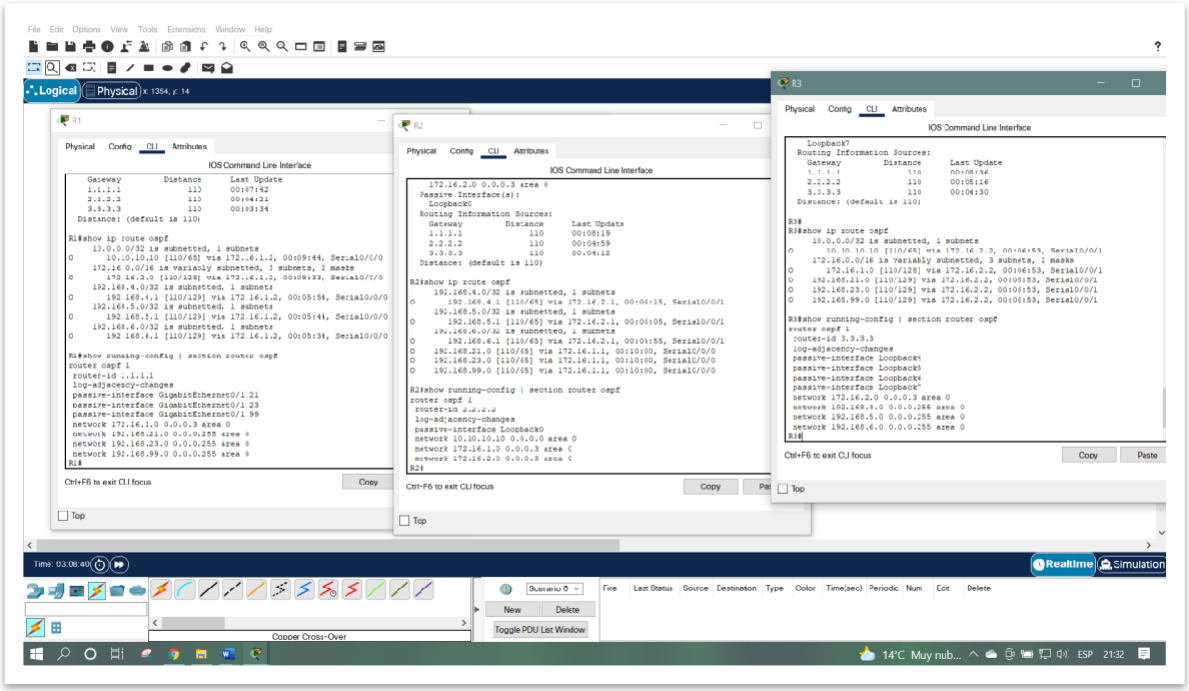
network 192.168.4.0 0.0.0.255 area 0

network 192.168.5.0 0.0.0.255 area 0

network 192.168.6.0 0.0.0.255 area 0

R3#

figura 21. Ejecución del comando show running-config | section router ospf.



Fuente: Autor

Parte 5: Implementar DHCP y NAT para IPv4

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

Los comandos para la configuración DHCP en las VLAN en R1 fueron comprobados, según la tabla:

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: Autor

Se configuro en R1 teniendo en cuenta la tabla 22, en este paso se hizo la configuración de DHCP en las VLAN, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R1#conf ter ingreso a modo de configuración

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 Añade una red a la cofiguracion OSPF

R1(dhcp-config)#default-router 192.168.21.1 router por defecto

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#domain-name ccna-sa.com Configura el nombre del dominio

R1(dhcp-config)#Ip dhcp pool ENGNR

R1(dhcp-config)#network 192.168.23.0 255.255.255.0 Añade una red a la configuración OSPF

R1(dhcp-config)#default-router 192.168.23.1 router por defecto

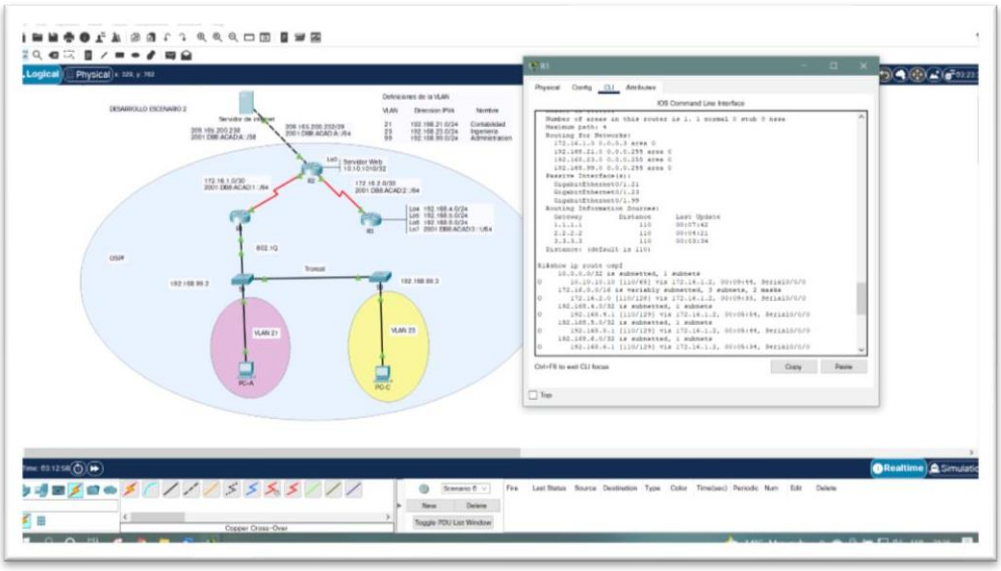
R1(dhcp-config)#dns-server 10.10.10.10

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

R1(dhcp-config)#exit

R1(config)#

figura 13. Ejecución de los comandos para configuración de DHCP R1.



Fuente**:** Autor

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

Los comandos para la configuración NAT estática y dinámica en el R2 fueron comprobados, según la tabla:

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: Autor

Se configuro en R2 teniendo en cuenta la tabla 22, en este paso se hizo la configuración de NAT estática y dinámica, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R2>enable inicio al modo privilegio

Password: contraseña

R2#conf ter inreso a modo de configuracion

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

R2(config)#username webuser privilege 15 secret cisco12345

R2(config)#ip http server configuracion de la ip del servidor

^

% 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

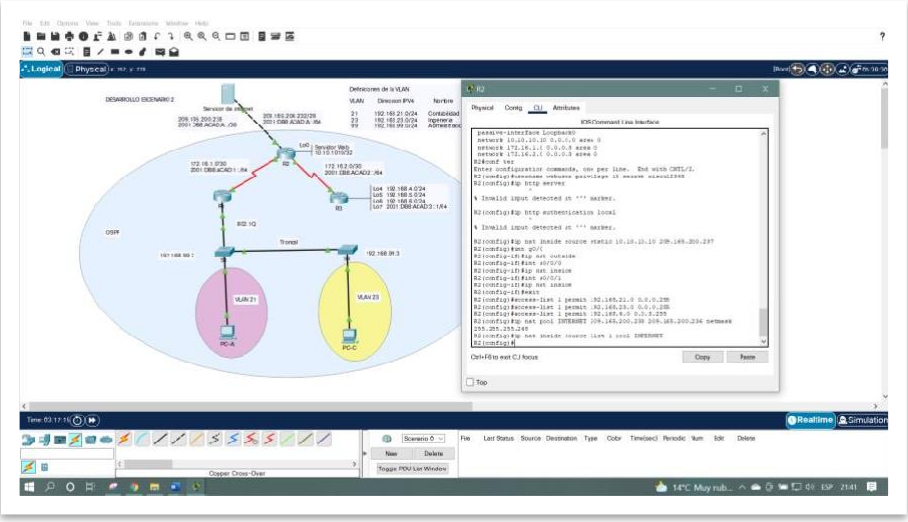
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255

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 14. Configuración de NAT estática y dinámica.



Fuente: Autor

Paso 3: Verificar el protocolo DHCP y la NAT estática

En la configuración de DHCP y NAT estática se hicieron las respectivas verificaciones, con el objetivo de mostrar el adecuado funcionamiento, el cual se muestra en la siguiente tabla:

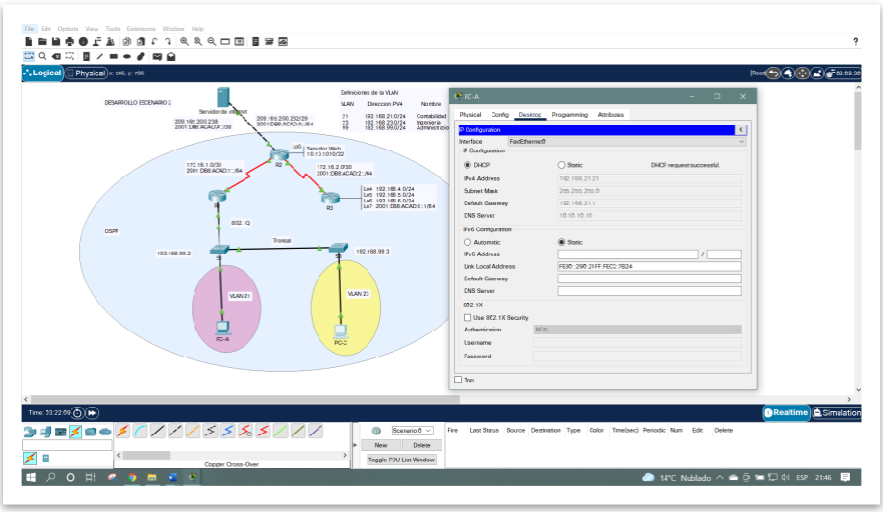
Tabla 24. Verificación de las configuraciones DHCP y NAT.

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: Autor

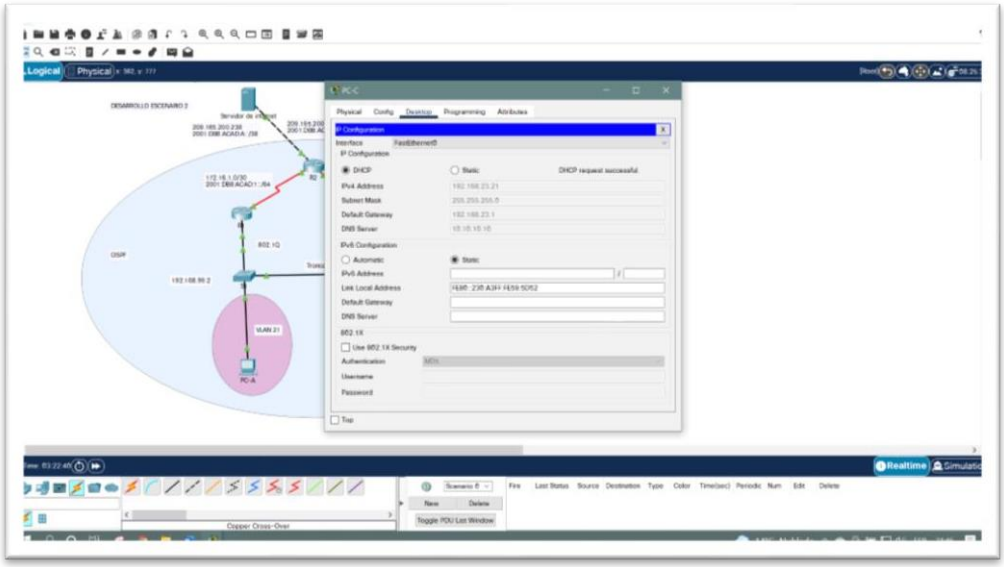
La configuración de DHCP y NAT estática se hicieron la respectiva comprobación, y sus resultados fueron los esperados como se muestra abajo:

figura 15. Resultados de la configuración DHCP en la PC-A.



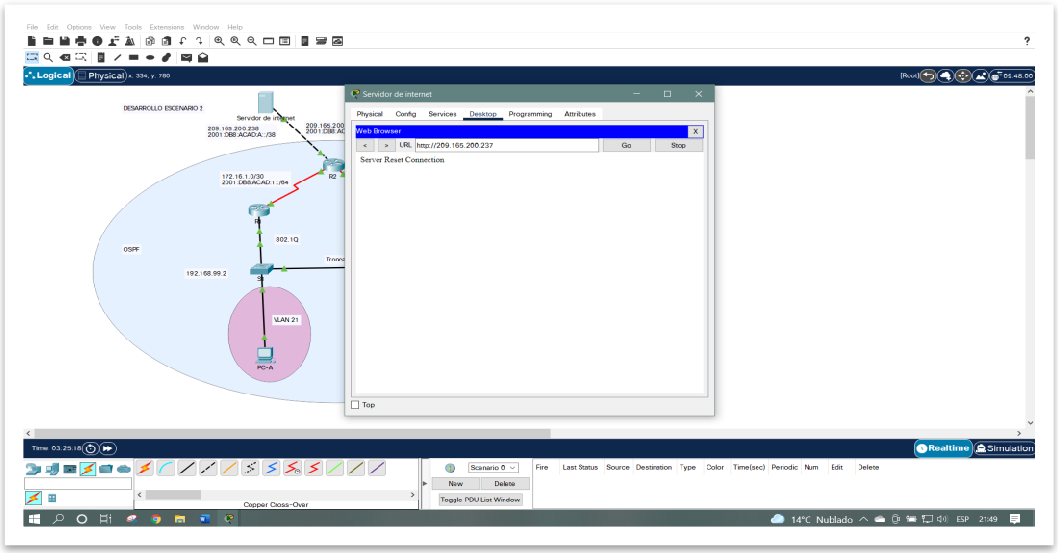
Fuente: Autor

figura 16. Resultados de la configuración DHCP en la PC-C.



Fuente: Autor

figura 17. Resultados de la configuración servicio web.



Fuente: Autor

Parte 6: Configurar NTP

Los comandos para la configuración NTP en el R2 y R1 fueron verificados según la siguiente tabla:

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: Autor

Se configuro en R2 y R1 teniendo en cuenta la tabla 25, en este paso se hizo la configuración de NAT, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

R2>enable inicio al modo privilegiado

Password: contraseña

R2#Clock set 14:05:30 10 november 2021 Configura los parámetros de hora del sistema en el switch

R2#conf ter ingreso a modo de configuracion

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

R2(config)#Ntp master 5

R2(config)#exit cerrar sesión

R2#

R1>enable inicio al modo privilegiado

Password: contraseña

R1#conf ter ingresando a modo de configuracion

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

R1(config)#ntp server 172.16.1.2

R1(config)#ntp update-calendar configuración de la fecha

R1(config)#end finalizer session

R1#

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

R1#

Verifique la configuración de NTP en R1.

R1#show ntp associations

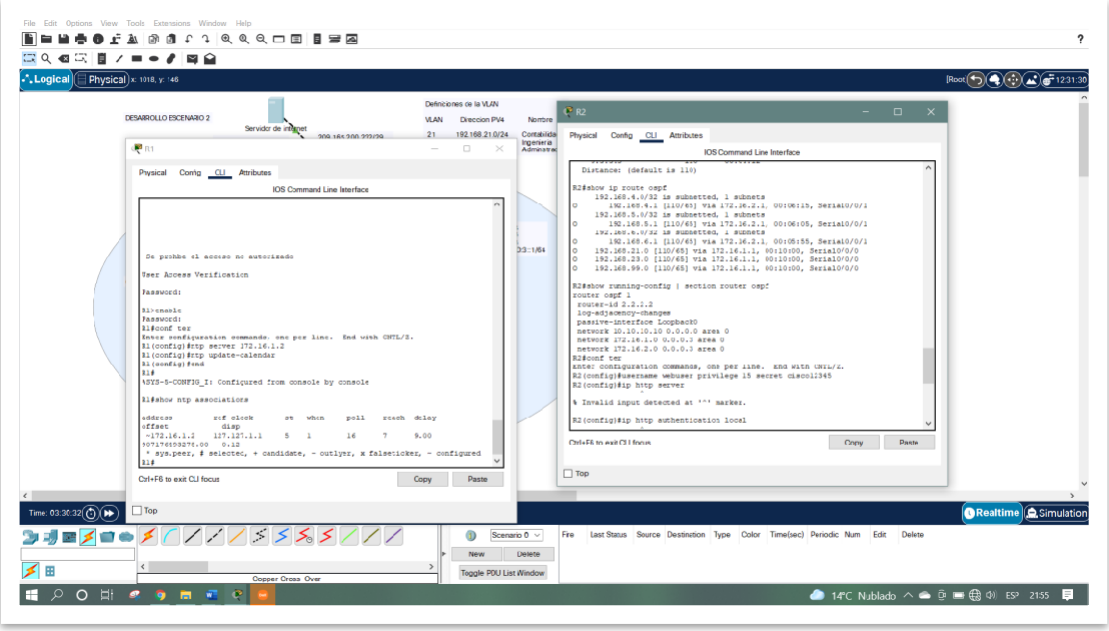
address ref clock st when poll reach delay offset disp

*~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 18. Configuración y ejecución de los comandos en R2 y R1.



Fuente: Autor

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

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

Los comandos para la configuración de restricción del acceso a las líneas VTY en el R2 fueron comprobadas, según la tabla:

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: Autor

Se configuro en R2 teniendo en cuenta la tabla 26, en este paso se hizo la configuración de la restricción del acceso a las líneas VTY en el R2, teniendo en cuenta el requerimiento de la topología, el cual lo podemos observar.

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 Salir sesión

R2(config)#line vty 0 4

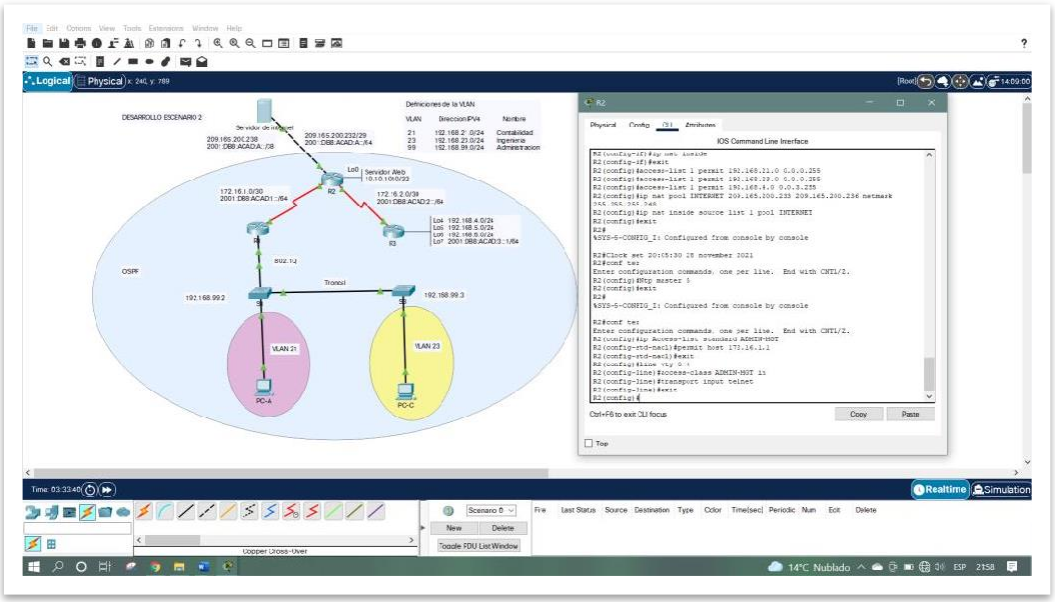
R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#transport input telnet configurar acceso remote telnet

R2(config-line)#exit cerrar sesión

R2(config)#

figura 19. Configuración de restricción de acceso líneas VTY en R2.



Fuente: Autor

En la configuración desde R1, se hace la verificación, donde obtenemos estos resultados:

Password: contraseña

R1>enable inicio al modo privilegiado

Password: contraseña

R1#telnet 172.16.1.2

Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado

User Access Verification

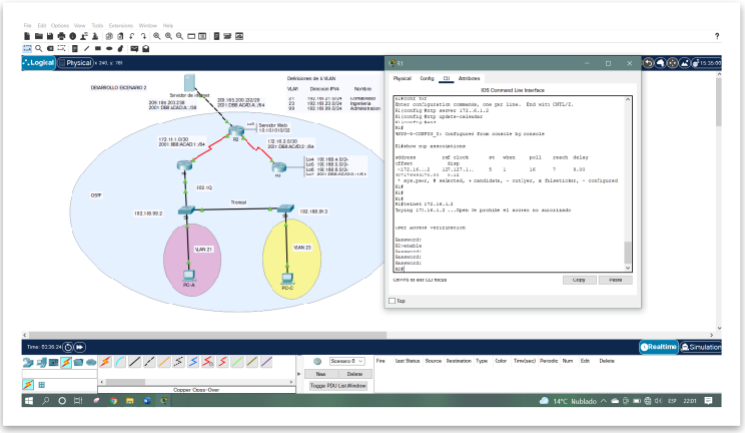
Password: contraseña

R2>enable inicio al modo privilegiado

Password: contraseña

R2#

figura 20. Verificación de la configuración Telnet desde R1.



Fuente: Autor

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

En los comandos CLI se verificaron su adecuado funcionamiento, según la tabla:

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	R2# show ip interface R2#

dirección en que se aplica?	
¿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: Autor

Se comprobó la configuración de la red verificando los comandos de CLI teniendo como resultados los esperados, el cual se muestra a continuación:

El comando show access-lists es ejecutado.

R2#show access-lists **Muestra el acceso de listas**
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#

El comando show ip interface fue ejecutado

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#

El comando show ip nat translations fue ejecutado:

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

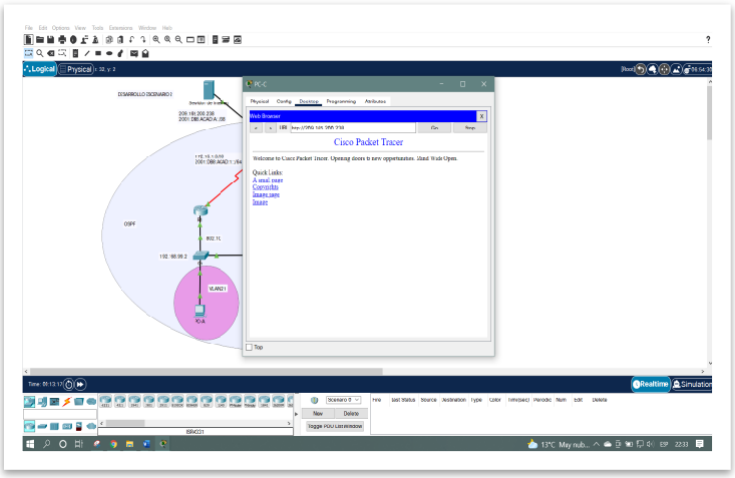
C:\>ping 209.165.200.238
Pinging 209.165.200.238 with 32 bytes of data:
Reply from 209.165.200.238: bytes=32 time=11ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=12ms TTL=126
Reply from 209.165.200.238: bytes=32 time=6ms TTL=126
Ping statistics 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 21. Ejecución del comando http://209.165.200.238.



Fuente: Autor

CONCLUSIONES

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

Se puede decir que packet tracer es una excelente herramienta, utilizada para hacer simulación en el aprendizaje de redes en forma virtual cuando no se tiene los equipos de comunicaciones en físico. Este simuador tiene una gran variedad de herramientas con las cuales se simula varias situaciones de la vida diaria. Por ultimo, utilizar el simulador packet tracer no se compara con la conexiónes en la vida real.

En conclusión, se cumplió con el objetivo de poner en práctica sobre los conocimientos adquiridos en el Diplomado De Profundización CISCO. Se pudo poner en práctica el manejo de redes, el cual se aplicó en los dos escenarios, y al mismo tiempo se construyó su respectiva topología en packet tracer.

Finalmente se tiene satisfacción por el aprendizaje adquirido durante el desarrollo del diplomado y la aplicación de la teoría vista de 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

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

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. " 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. "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. "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. "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

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, *12*(1), 86-93.