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

DIANA ISABEL MEDINA SANTAMARIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
DUITAMA - BOYACA
2021

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

DIANA ISABEL MEDINA SANTAMARIA

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

DIRECTOR:
MSc. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
DUITAMA - BOYACA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Duitama, Boyacá, noviembre de 2021

AGRADECIMIENTOS

Agradezco a cada una de las personas que han sido parte de este camino en mis años de estudio, mi familia, tutores, compañeros de los cuales he aprendido mucho y recibido todo el apoyo para estar hoy culminando mi carrera profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Conmutación: La Conmutación se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

Enrutamiento: El proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

Redes: La interconexión de un número determinado de computadores (o de redes, a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado.

Dirección IP: Una dirección IP es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Ping: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

DHCP: El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada

Router: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Switch: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

RESUMEN

El presente trabajo muestra el desarrollo de la prueba de habilidades de CISCO CCNA con la configuración de dispositivos en dos escenarios propuestos, demostrando el nivel de conocimiento adquirido en el transcurso del diplomado. A través de la simulación en Packet Tracer se implementa la topología del escenario 1 y escenario 2, detallando paso a paso los comandos utilizados; en el escenario 1 se creó el diseño ipv4 para las LAN propuestas, configuración básicas de dispositivos de la red, ajustes de seguridad básicos como contraseñas y cifrado de las mismas, configuración de host y verificación de la conectividad de la red; en el escenario 2 se configuro una red que admita ipv4 e ipv6, configuración básica y de seguridad de Routers y Switchs, creación de Vlans y enrutamiento entre estás, configuración de protocolo DHCP para asignación dinámica de direcciones IP en los host, configuración protocolo OSPF para enlace de la red, traducción de direcciones dinámicas y estáticas mediante el protocolo NAT y listas de control de acceso (ACL) para brindar mayor seguridad a la red. Al realizar los escenarios con todas sus configuraciones obtuvimos redes con conectividad en todos los equipos, seguridad y funcionalidad.

Palabras clave: Redes, Router, Switch, Ping, Enrutamiento, Ipv6, Ipv4.

ABSTRACT

This work shows the development of the CISCO CCNA skills test with the configuration of devices in two proposed scenarios, demonstrating the level of knowledge acquired in the course of the diploma. Through the simulation in Packet Tracer, the topology of scenario 1 and scenario 2 is implemented, detailing the commands used step by step; In scenario 1, we were able to create the ipv4 design for the proposed LANs, basic configuration of network devices, basic security settings such as passwords and their encryption, host configuration and verification of network connectivity; In scenario 2, a network that supports ipv4 and ipv6 was configured, basic and security configuration of Routers and Switches, creation of Vlans and routing between these, configuration of DHCP protocol for dynamic assignment of IP addresses in hosts, configuration of OSPF protocol for network binding, static and dynamic address translation using NAT protocol, and access control lists (ACLs) to provide increased network security. When carrying out the scenarios with all their configurations, we obtained networks with connectivity in all the equipment, security and functionality.

Keywords: Networks, Router, Switch, Ping, Routing, Ipv6, Ipv4.

INTRODUCCION

Con el análisis y desarrollo de la prueba de habilidades CCNA, se ponen en práctica todos los conocimientos adquiridos durante el estudio del diplomado de profundización. Por medio de herramientas de simulación como Packet Tracer donde se realiza la topología de dos escenarios, conectando varios dispositivos, realizando la configuración correspondiente según los requerimientos que nos indican.

A continuación, se encontrará el desarrollo del escenario inicial propuesto, donde se avanzará en las habilidades de configuración de dispositivos como Router, Swich y Pc, a través de direccionamiento IP, comandos de configuración de aspectos básicos, de seguridad y verificación de conectividad entre equipos.

Luego se encontrará el desarrollo del escenario dos, realizando las configuraciones requeridas según la topología de red paso a paso, avanzando en temas como enrutamiento estático y dinámico bajo direccionamiento IP para dar soluciones de conectividad, creación de vlans para comprender mejor el uso de estas en las redes para administrar varios dominios en una misma red, uso del protocolo DHCP para generar seguridad al acceder a la red y traducción de direcciones IP públicas o privadas generando máxima seguridad con el uso de NAT- PAT.

ESCENARIO 1

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

Figura 1. Escenario 1

Fuente propia

Parte 2: Desarrolle el esquema de direccionamiento IP

Tabla 1. Tabla de Direccionamiento

Item	Requerimiento
Dirección de Red	192.168.77.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.77.1/25
R1 G0/0/0	192.168.77.129/26
S1 SVI	192.168.77.2/25
PC-A	192.168.77.126/25
PC-B	192.168.77.190/26

Fuente propia

Parte 3: Configurar aspectos básicos R1 mediante conexión de consola

Router 1

Router>enable *//Acceso a modo EXEC privilegiado*
Router#configure terminal *//Ingreso a modo configuración*
Router(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Router(config)#hostname R1 *//Comando para nombrar Router*

R1(config)#ip domain-name ccna-lab.com *//Comando para nombre de dominio*
R1(config)#enable secret ciscoenpass *//Comando para contraseña cifrada en EXEC privilegiado*
R1(config)#line console 0 *//Acceso a la consola*
R1(config-line)#password ciscoconpass *//Contraseña de acceso a la consola*
R1(config-line)#login *//Autenticación al iniciar sesión*
R1(config-line)#exit *//Salir de modo line*
R1(config)#security password min-length 10 *//Establecer longitud minina para contraseñas*
R1(config)#username admin password admin1pass *//Comando crear usuario admin en la base de datos local*
R1(config)#line vty 0 4 *//Comando ingreso a VTY*
R1(config-line)#password cisco *//Comando password, como la password es de menos de 10 caracteres nos sale el siguiente mensaje:*
% Password too short - must be at least 10 characters. Password not configured.
R1(config-line)#password ciscocisco *//Comando para colocar contraseña*
R1(config-line)#login local *//Comando para autenticación local iniciar sesión*
R1(config-line)#transport input SSH *//Comando para configurar VTY aceptando SSH*
R1(config-line)#exit *//Salir de modo VTY*
R1(config)#service password-encryption *//Comando para cifrar contraseñas*
R1(config)#banner motd #Este es el router de la UNAD, acceso no permitido# *//Comando configurar motd banner*
R1(config)#interface G0/0/0 *//Configurar interfaz G0/0/0*
R1(config-if)#ip address 192.168.77.129 255.255.255.192 *//Comando para establecer dirección ipv4 y mascara de subred*
R1(config-if)#description Esta es la interfaz de la LAN2 *//Comando para descripción de configuración*
R1(config-if)#no shutdown *//Comando para habilitar la interfaz*

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)#exit *//Salir de configuración de interfaz*
R1(config)#interface G0/0/1 *//Configurar interfaz G0/0/1*
R1(config-if)#ip address 192.168.77.1 255.255.255.128 *//Comando para establecer dirección ipv4 y mascara de subred*
R1(config-if)#description Esta es la interfaz de la LAN1 *//Comando para descripción de configuración*
R1(config-if)#no shutdown *//Comando para habilitar la interfaz*

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 *//Salir de configuración de interfaz*
R1(config)#ip domain name ccna-lab.com *//Comando para nombre de dominio*
R1(config)#crypto key generate rsa *//Comando para generar clave de cifrado 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 *//Ingreso de modulo de bits que se desea*
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#exit
*Mar 1 2:11:5.92: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr *//Guardamos configuración*
Building configuration...
[OK]
R1#

Parte 4: Configurar aspectos básicos S1 mediante conexión de consola

Switch 1

Switch>enable *//Acceso a modo EXEC privilegiado*
Switch#configure terminal *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Switch(config)#hostname S1 *//Comando para nombrar Switch*
S1(config)#ip domain-name ccna-lab.com *//Comando para nombre de dominio*
S1(config)#enable secret ciscoenpass *//Comando para contraseña cifrada en EXEC privilegiado*
S1(config)#line console 0 *//Acceso a la consola*
S1(config-line)#password ciscoconpass *//Contraseña de acceso a la consola*
S1(config-line)#login *//Autenticación al iniciar sesión*
S1(config-line)#exit *//Salir de modo line*
S1(config)#username admin password admin1pass *//Comando crear usuario admin en la base de datos local*
S1(config)#line vty 0 15 *//Comando ingreso a VTY*
S1(config-line)#password ciscocisco *//Comando para colocar contraseña*
S1(config-line)#login local *//Comando para autenticación local iniciar sesión*

S1(config-line)#transport input SSH *//Comando para configurar VTY aceptando SSH*
S1(config-line)#exit *//Salir de modo VTY*
S1(config)#service password-encryption *//Comando para cifrar contraseñas*
S1(config)#banner motd #Este es el Switch de la UNAD, acceso no permitido# *//Comando configurar motd banner*
S1(config)#ip domain name ccna-lab.com *//Comando para nombre de dominio*
S1(config)#crypto key generate rsa *//Comando para generar clave de cifrado RSA*
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024 *//Ingreso de módulo de bits que se desea*
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#interface vlan 1 *//Configurar interfaz Vlan1*
*Mar 1 2:28:25.109: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.77.2 255.255.255.128 *//Comando para establecer dirección ipv4 y mascara de subred*
S1(config-if)#no shutdown *//Comando para habilitar la interfaz*

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config)#ip default-gateway 192.168.77.1 Comando configuración Gateway predeterminado
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#wr *Guardamos configuración*
Building configuration...
[OK]

Parte 5. Configurar los equipos
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

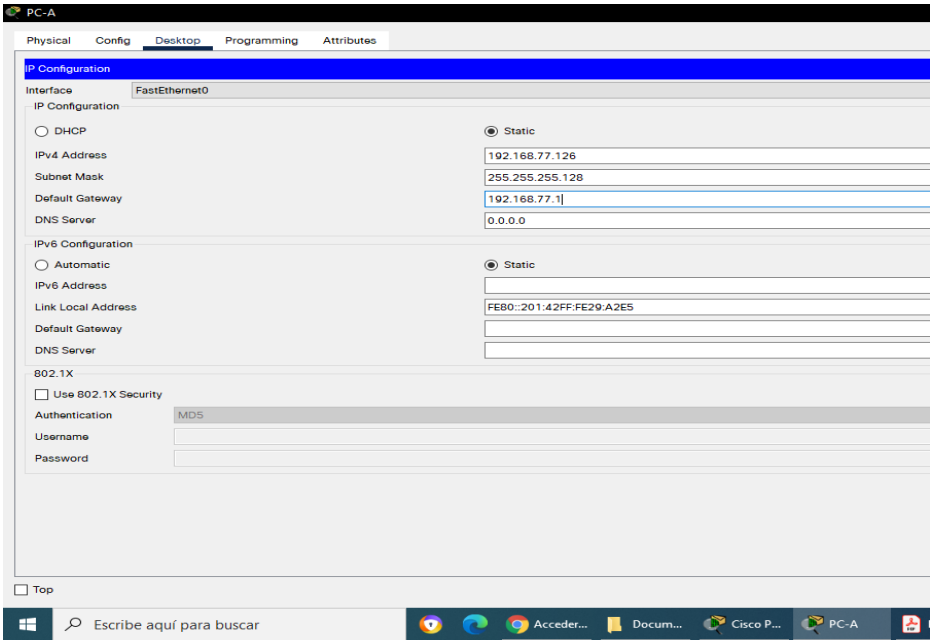
PC-A

Tabla 2. Configuración PC-A

Network Configuration	
Descripción	*PC- A*
Dirección física	001.4229.A2E5
Dirección IP	192.168.77.126/25
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.77.1

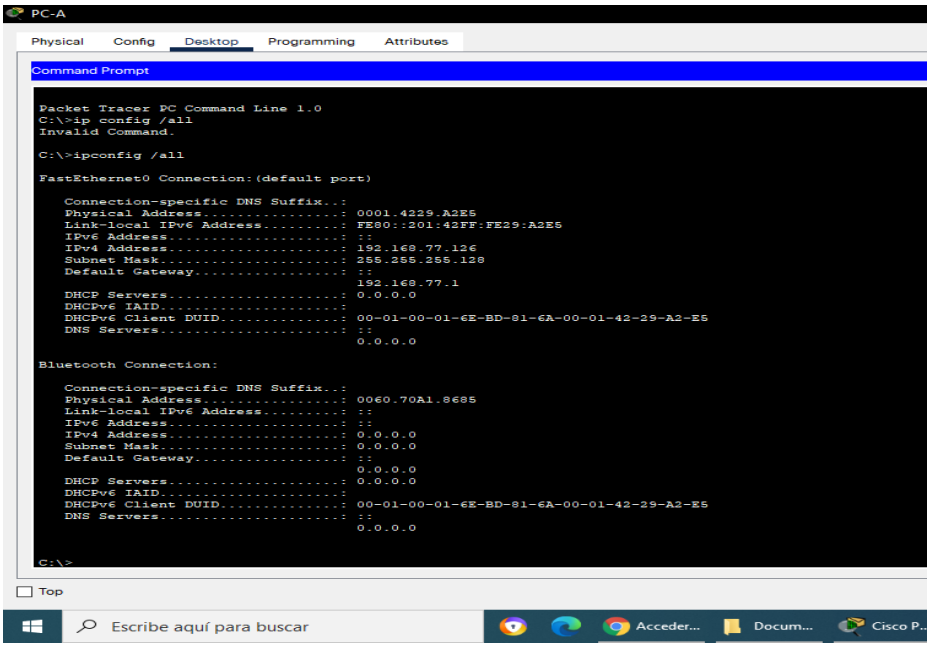
Fuente propia

Figura 2. Configuración PC-A



Fuente propia

Figura 3. Comando ip config /all PC-A



Fuente propia

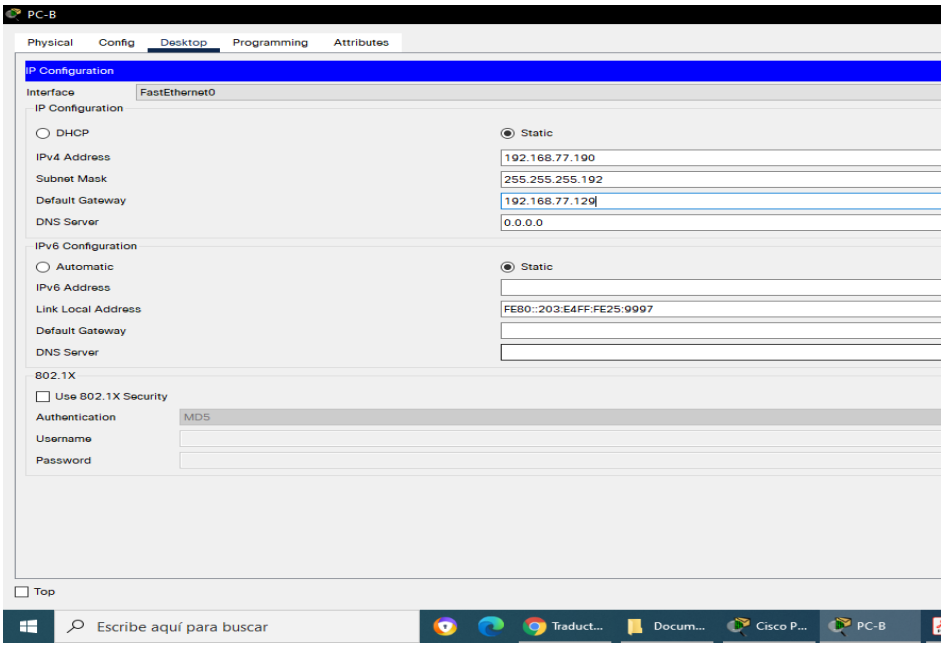
PC-B

Tabla 3. Configuración PC-B

Network Configuration	
Descripción	*PC- B*
Dirección física	003. E425.9997
Dirección IP	192.168.77.190/26
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.77.129

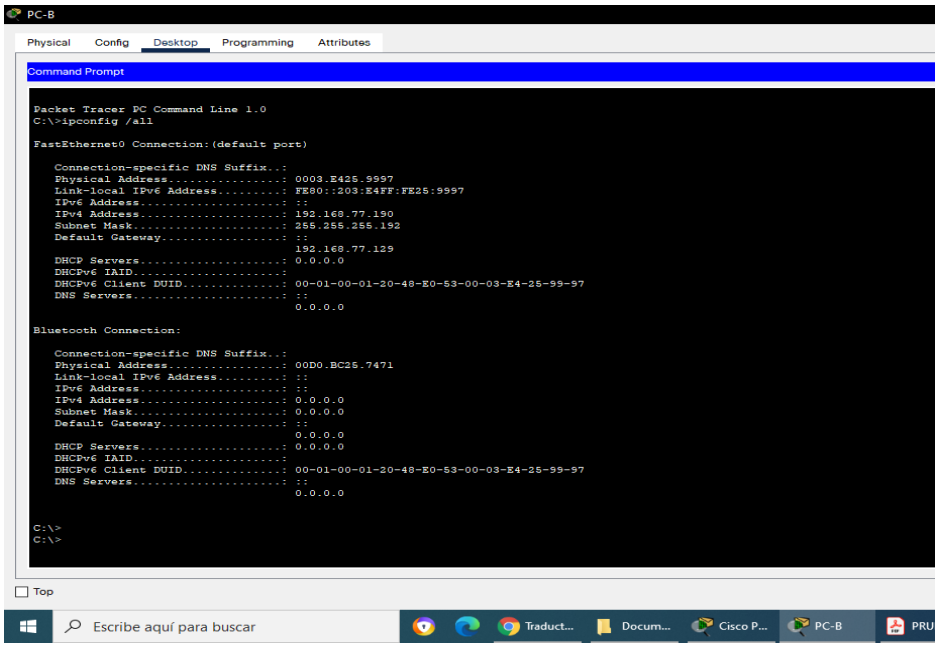
Fuente propia

Figura 4. Configuración PC-A



Fuente propia

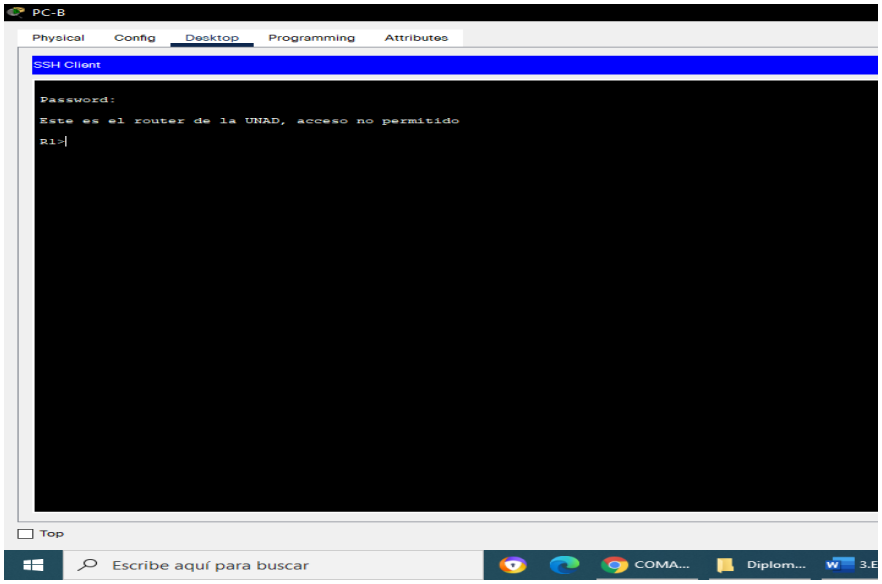
Figura 5. Comando ip config /all PC-B



Fuente propia

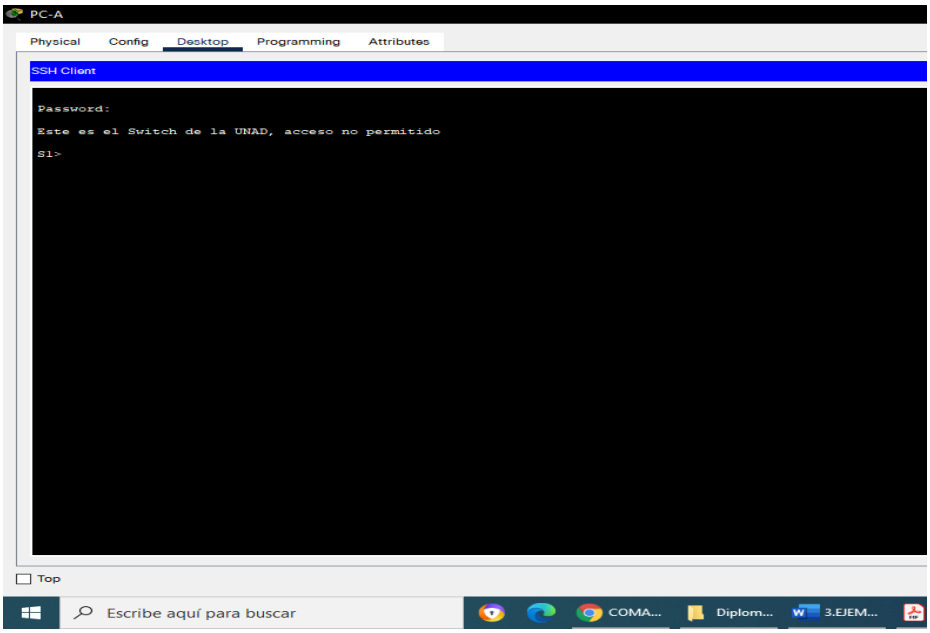
Parte 6. Verificación de conectividad

Figura 6. Verificación conectividad SSH Router



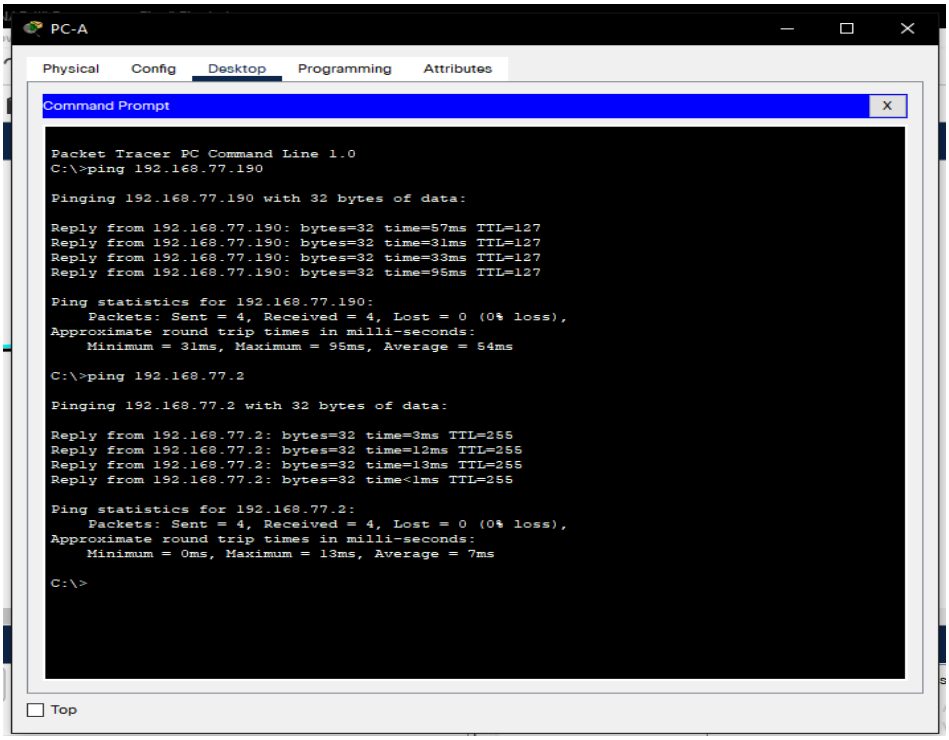
Fuente propia

Figura 7. Verificación conectividad SSH Switch



Fuente propia

Figura 8. Comando ping entre equipos



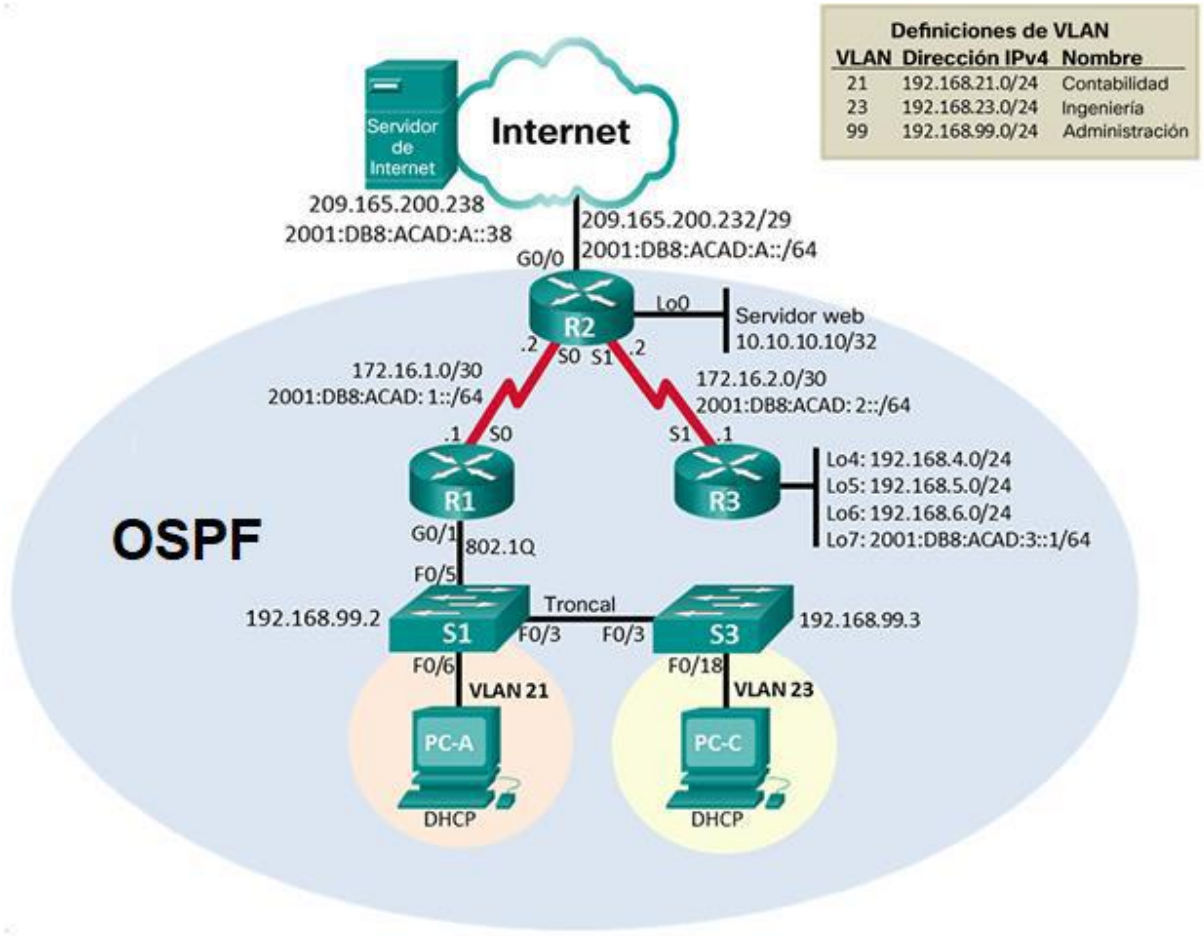
Fuente propia

ESCENARIO 2

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

Topología

Figura 9. Topología Escenario 2



Fuente Prueba de habilidades CCNA II-2021

Parte 1: Inicializar dispositivos

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

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

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

Tabla 4. Comando de inicialización de dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show vlan

Fuente propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

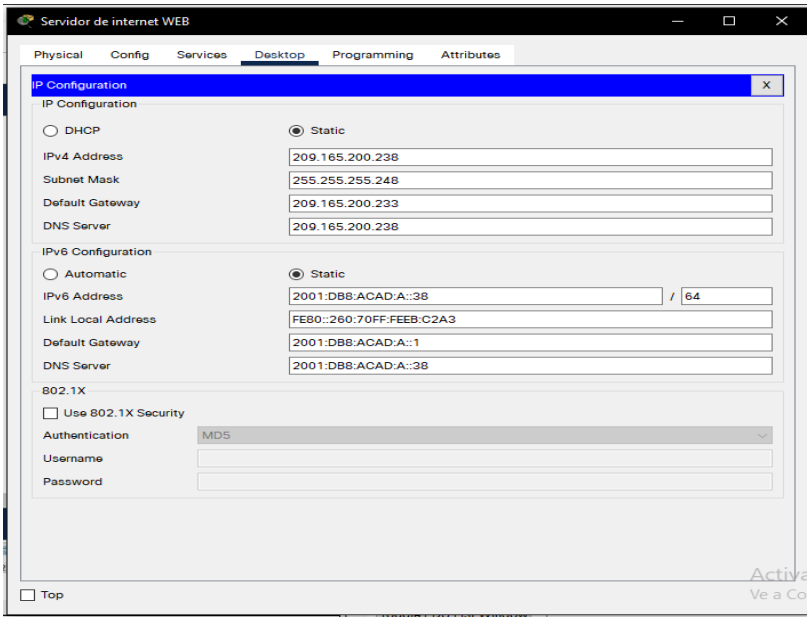
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 5. Configuración servidor de internet

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

Fuente propia

Figura 10. Configuración Servidor de internet



Fuente propia

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 6. Configuracion Router1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Fuente propia

ROUTER R1

Router>enable *//Acceso a modo EXEC privilegiado*
Router#configure terminal *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Router(config)#hostname R1 *//Comando para nombrar Router*
R1(config)#enable secret class *//Comando para contraseña cifrada en EXEC privilegiado*
R1(config)#line console 0 *//Acceso a la consola*
R1(config-line)#password cisco *//Contraseña de acceso a la consola*
R1(config-line)#login *//Autenticación al iniciar sesión*
R1(config-line)#exit *//Salir de modo de configuración*
R1(config)#line vty 0 4 *//Comando ingreso a VTY*
R1(config-line)#password cisco *//contraseña de acceso a telnet*
R1(config-line)#login local *//Comando para autenticación local iniciar sesión*
R1(config-line)#exit *//Salir de modo de configuración*
R1(config)#service password-encryption *//Comando para cifrar contraseñas*
R1(config)#banner motd #Se prohibe el acceso no autorizado# *//Mensaje de acceso al router*
R1(config)#ipv6 unicast-routing *//Activación del protocolo IPV6 a nivel global*
R1(config)#interface serial0/2/0 *//Configurar interfaz*
R1(config-if)#description R1 a R2 *// Descripcion interfaz s0/2/0*
R1(config-if)#ip address 172.16.1.1 255.255.255.252 *//Comando para establecer dirección ipv4 y mascara de subred*

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 *//Comando para establecer dirección ipv6*
R1(config-if)#clock rate 128000 *//Establecer la frecuencia de reloj en 128000*
R1(config-if)#no shutdown *//Comando para habilitar la interfaz*

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to down
R1(config-if)#exit *//Salir de modo de configuración*
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 0 *//Configuración rutas predeterminadas ipv4 en S0/2/0*
R1(config)#ipv6 route ::/0 s0/2/0 *//Configuración rutas predeterminadas ipv6*
R1(config)#ipv6 unicast-routing *// Habilitar routing ipv6*
R1(config)#exit *//Salir de modo de configuración*

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas

Tabla 7. Configuración Router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	No soportado en packet tracer
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz

Fuente propia

ROUTER 2

Router>enable *//Acceso a modo EXEC privilegiado*
Router#configure terminal *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Router(config)#hostname R2 *//Comando para nombrar Router*

R2(config)#enable secret class *//Comando para contraseña cifrada en EXEC privilegiado*
R2(config)#line console 0 *//Acceso a la consola*
R2(config-line)#password cisco *//Contraseña de acceso a la consola*
R2(config-line)#login *//Autenticación al iniciar sesión*
R2(config-line)#exit *//Salir de modo de configuración*
R2(config)#line vty 0 4 *//Comando ingreso a VTY*
R2(config-line)#password cisco *//contraseña de acceso a telnet*
R2(config-line)#login local *//Comando para autenticación local iniciar sesión*
R2(config-line)#exit *//Salir de modo de configuración*
R2(config)#service password-encryption *//Comando para cifrar contraseñas*
//habilitación para Servidor HTTP no soportado en packet tracer
R2(config)#ip http server
R2(config)#ip http secure-server
R2(config)# ip http authentication local

R2(config)#banner motd #Se prohibe el acceso no autorizado# *//Mensaje de acceso al router*
R2(config)#ipv6 unicast-routing *//Activación del protocolo IPV6 a nivel global*
R2(config)#interface serial 0/2/0 *//Configurar interfaz*
R2(config-if)#description R1 a R2 *//Descripción interfaz s0/2/0*
R2(config-if)#ip address 172.16.1.2 255.255.255.252 *//Comando para establecer dirección ipv4 y mascara de subred*
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 *//Comando para establecer dirección ipv6*
R2(config-if)#no shutdown *//Comando para habilitar la interfaz*

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

R2(config-if)#exit *//Salir de modo de configuración*
R2(config)#interface serial 0/2/1 *//Configurar interfaz*
R2(config-if)#description R2 a R3 *//Descripción interfaz s0/2/1*
R2(config-if)#ip address 172.16.2.2 255.255.255.252 *//Comando para establecer dirección ipv4 y mascara de subred*
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 *//Comando para establecer dirección ipv6*
R2(config-if)#clock rate 128000 *//Establecer la frecuencia de reloj en 128000*
R2(config-if)#no shutdown *//Comando para habilitar la interfaz*

R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0/0 *//Configurar interfaz*
R2(config-if)#description R2 a internet *//Descripción interfaz gi0/0/0*
R2(config-if)#ip address 209.165.200.233 255.255.255.248 *//Comando para establecer dirección ipv4 y mascara de subred*
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 64 *//Comando para establecer dirección ipv6*
R2(config-if)#no shutdown *//Comando para habilitar la interfaz*

R2(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

R2(config-if)#exit *//Salir de modo de configuración*
R2(config)#interface lo0 *//Configurar interfaz*

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)#ip address 10.10.10.10 255.255.255.255 *//Comando para establecer dirección ipv4 y mascara de subred*
R2(config-if)#exit *//Salir de modo de configuración*

//Configuración rutas predeterminadas ipv4 e ipv6
R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0/0 *//Ruta predeterminada ipv4*
R2(config)#ipv6 route ::/0 gigabitEthernet 0/0/0 *//Ruta predeterminada ipv6*
R2(config)#ipv6 unicast-routing *//Habilitar routing ipv6*
R2(config)#exit *//Salir de modo de configuración*

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 8. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco

Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Fuente propia

ROUTER 3

Router>enable *//Acceso a modo EXEC privilegiado*
Router#configure terminal *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Router(config)#hostname R3 *//Comando para nombrar Router*
R3(config)#enable secret class *//Comando para contraseña cifrada en EXEC privilegiado*
R3(config)#line console 0 *//Acceso a la consola*
R3(config-line)#password cisco *//Contraseña de acceso a la consola*
R3(config-line)#login *//Autenticación al iniciar sesión*
R3(config-line)#exit *//Salir de modo de configuración*
R3(config)#line vty 0 4 *//Comando ingreso a VTY*
R3(config-line)#password cisco *//contraseña de acceso a telnet*

R3(config-line)#login local *//Comando para autenticación local iniciar sesión*
R3(config-line)#exit *//Salir de modo de configuración*
R3(config)#service password-encryption *//Comando para cifrar contraseñas*
R3(config)#banner motd #Se prohibe el acceso no autorizado# *//Mensaje de acceso al router*
R3(config)#ipv6 unicast-routing *//Activación del protocolo IPV6 a nivel global*
R3(config)#interface serial0/2/1 *//Configurar interfaz*

R3(config-if)#description R3 a R2 //Descripcion S0/2/1
R3(config-if)#ip address 172.16.2.1 255.255.255.252 //*Comando para establecer dirección ipv4 y mascara de subred*
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 //*Comando para establecer dirección ipv6*
R3(config-if)#no shutdown //*Comando para habilitar la interfaz*

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

R3(config-if)#exit *//Salir de modo de configuración*
R3(config)#interface lo4 //*Configurar y crear interfaz lo4*

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0 //*Comando para establecer dirección ipv4 y mascara de subred*
R3(config-if)#exit *//Salir de modo de configuración*
R3(config)#interface lo5 //*Configurar y crear interfaz lo5*

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

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

R3(config-if)#ip address 192.168.5.1 255.255.255.0 //*Comando para establecer dirección ipv4 y mascara de subred*
R3(config-if)#exit *//Salir de modo de configuración*

R3(config)#interface lo6 //*Configurar y crear interfaz lo6*

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

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

R3(config-if)#ip address 192.168.6.1 255.255.255.0 0 *//Comando para establecer dirección ipv4 y mascara de subred*
R3(config-if)#exit *//Salir de modo de configuración*
R3(config)#interface lo7 *//Configurar y crear interfaz lo7*

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up

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

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 *//Comando para establecer dirección ipv6*
R3(config-if)#exit *//Salir de modo de configuración*

//Configuración rutas predeterminadas ipv4 e ipv6
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1 *//Ruta predeterminada ipv4*
R3(config)#ipv6 route ::/0 s0/2/1 *//Ruta predeterminada ipv6*
R3(config)#exit *//Salir de modo de configuración*

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configuración S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente propia

SWITCH 1

Switch>enable *//Acceso a modo EXEC privilegiado*
Switch#configure terminal *//Ingreso a modo configuración*
Switch(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Switch(config)#hostname S1 *//Comando para nombrar Router*
S1(config)#enable secret class *//Comando para contraseña cifrada en EXEC*

privilegiado
S1(config)#line console 0 *//Acceso a la consola*
S1(config-line)#password cisco *//Contraseña de acceso a la consola*
S1(config-line)#login *//Autenticación al iniciar sesión*
S1(config-line)#exit *//Salir de modo de configuración*
S1(config)#line vty 0 4 *//Comando ingreso a VTY*
S1(config-line)#password cisco *//contraseña de acceso a telnet*
S1(config-line)#login *//Comando para autenticación iniciar sesión*
S1(config-line)#exit *//Salir de modo de configuración*
S1(config)#service password-encryption *//Comando para cifrar contraseñas*
S1(config)#banner motd #Se prohibe el acceso no autorizado# *//Mensaje de acceso al router*

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente propia

SWITCH 3

Switch>enable *//Acceso a modo EXEC privilegiado*
Switch#configure terminal *//Ingreso a modo configuración*
Switch(config)#no ip domain-lookup *//Comando para desactivar búsqueda DNS*
Switch(config)#hostname S3 *//Comando para nombrar* Switch
S3(config)#enable secret class *//Comando para contraseña cifrada en EXEC privilegiado*
S3(config)#line console 0 *//Acceso a la consola*
S3(config-line)#password cisco *//Contraseña de acceso a la consola*
S3(config-line)#login *//Autenticación al iniciar sesión*
S3(config-line)#exit *//Salir de modo de configuración*
S3(config)#line vty 0 4 *//Comando ingreso a VTY*

S3(config-line)#password cisco *//Contraseña de acceso a telnet*
S3(config-line)#login *//Comando para autenticación iniciar sesión*
S3(config-line)#exit *//Salir de modo de configuración*
S3(config)#service password-encryption *//Comando para cifrar contraseñas*
S3(config)#banner motd #Se prohibe el acceso no autorizado# *//Mensaje de acceso al switch*

Paso 7: Verificar la conectividad de la red

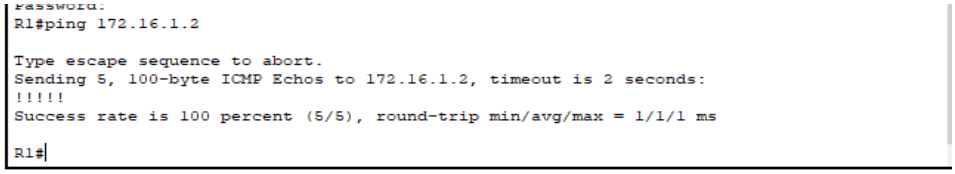
Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 11. Verificación conectividad de red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/23 ms
PC de Internet	Gateway predeterminado		Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

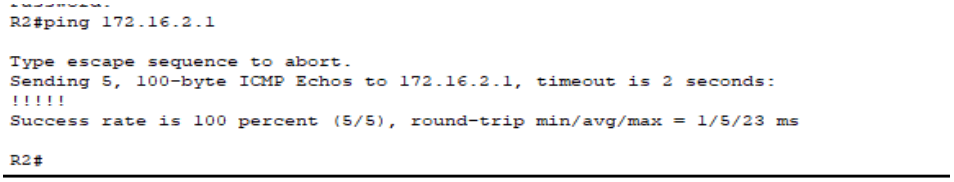
Fuente propia

Figura 11. Ping de R1 a R2



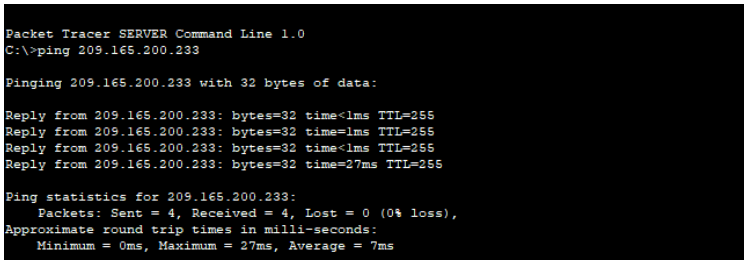
Fuente propia

Figura 12. Ping de R2 a R3



Fuente propia

Figura 13. Ping de Pc de internet a Gateway predeterminado



Fuente propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración de S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican

Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente propia

Switch 1

S1#enable *//Acceso a modo EXEC privilegiado*
S1#configure terminal *//Ingreso a modo configuración*

// Crear y nombrar cada una de las Vlan como se muestra en la topología
S1(config)#vlan 21 *//Creación Vlan 21*
S1(config-vlan)#name Contabilidad *//Asignación nombre vlan 21*
S1(config-vlan)#vlan 23 *//Creacion Vlan 23*
S1(config-vlan)#name Ingenieria *//Asignación nombre vlan 23*
S1(config-vlan)#vlan 99 *//Creacion Vlan 99*
S1(config-vlan)#name Administración *//Asignación nombre vlan 99*
S1(config-vlan)#exit *//Salir de modo de configuración*
S1(config)#interface vlan 99 *//Configurar interfaz vlan 99*
S1(config-if)#ip address 192.168.99.2 255.255.255.0 *//Asignación dirección ipv4 y mascara de subred para vlan 99*
S1(config-if)#no shutdown *//Comando para habilitar la interfaz*
S1(config-if)#exit *//Salir de modo de configuración*
S1(config)#ip default-gateway 192.168.99.1 *//Asignación gateway predeterminado*

//Forzar el enlace troncal en la interfaz F0/3
S1(config)#interface FastEthernet 0/3 *//Configurar interfaz*
S1(config-if)#switchport mode trunk *//Creación enlace troncal*
S1(config-if)#switchport trunk native vlan 1 *//Asignación vlan 1 como vlan nativa*
S1(config-if)#exit *//Salir de modo de configuración*

//Forzar el enlace troncal en la interfaz F0/5
S1(config-if)#interface fastEthernet 0/5 *//Configurar interfaz*
S1(config-if)#switchport mode trunk //Creacion enlace troncal
S1(config-if)#switchport trunk native vlan 1 *//Asignación vlan 1 como vlan nativa*
S1(config-if)#exit *//Salir de modo de configuración*

//Configurar el resto de los puertos como puertos de acceso
S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 *//Ingreso rango interfaces*
S1(config-if-range)#switchport mode access *//Configuración interfaces como puertos de acceso*
S1(config-if-range)#exit *//Salir de modo de configuración*

//Asignar F0/6 a la VLAN 21
S1(config)#interface range fa0/6 *//Configurar interfaz*
S1(config-if-range)#switchport access vlan 21 *// Asignación fa0/6 a vlan 21*
S1(config-if-range)#exit *//Salir de modo de configuración*

//Apagar todos los puertos sin usar
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 *//Ingreso rango de interfaces sin usar*
S1(config-if-range)#shutdown *//Apagar rango de interfaces sin usar*

S1(config-if-range)#exit *//Salir de modo de configuración*
Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Fuente propia

Switch 3

S3>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso contraseña*
S3#configure terminal *//Ingreso a modo configuración*

// Crear y nombrar cada una de las Vlan como se muestra en la topología
S3(config)#vlan 21 *//Creación Vlan 21*
S3(config-vlan)#name Contabilidad *//Asignación nombre vlan 21*
S3(config-vlan)#vlan 23 *//Creación Vlan 23*
S3(config-vlan)#name Ingeniería *//Asignación nombre vlan 23*
S3(config-vlan)#vlan 99 *//Creación Vlan 99*
S3(config-vlan)#name Administración *//Asignación nombre vlan 23*
S3(config-vlan)#exit *//Salir de modo de configuración*

S3(config)#interface vlan 99 *//Configurar interfaz*
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

S3(config-if)#ip address 192.168.99.3 255.255.255.0 *//Asignación dirección ipv4 y mascara de subred para vlan 99*
S3(config-if)#no shutdown *//Comando para habilitar la interfaz*
S3(config-if)#exit *//Salir de modo de configuración*
S3(config)#ip default-gateway 192.168.99.1 *//Asignación gateway predeterminado*

//Forzar el enlace troncal en la interfaz F0/3
S3(config)#interface fastEthernet 0/3 *//Configurar interfaz*
S3(config-if)#switchport mode trunk *//Creación enlace troncal*
S3(config-if)#switchport trunk native vlan 1 *//Asignación vlan 1 como vlan nativa*
S3(config-if)#exit *//Salir de modo de configuración*

//Configurar el resto de los puertos como puertos de acceso
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 *//Ingreso rango interfaces*
S3(config-if-range)#switchport mode access *//Configuración interfaces como puertos de acceso*
S3(config-if-range)#exit *//Salir de modo de configuración*

//Asignar F0/18 a la VLAN 21
S3(config)#interface FastEthernet 0/18 *//Configurar interfaz*
S3(config-if)#switchport access vlan 21 *// Asignación fa0/18 a vlan 21*
S3(config-if)#exit *//Salir de modo de configuración*

//Apagar todos los puertos sin usar
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 *//Ingreso rango de interfaces sin usar*
S3(config-if-range)#shutdown *//Apagar rango de interfaces sin usar*

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Fuente propia

Router 1

R1>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso contraseña*
R1#configure terminal *//Ingreso a modo configuración*

//Configuración de la subinterfaz 802.1Q.21 en Gi0/0/1
R1(config)#interface gigabitEthernet 0/0/1.21 *//Crear subinterfaz g0/0/1.21*
R1(config-subif)#description LAN de Contabilidad *//Descripción g0/0/1.21*
R1(config-subif)#encapsulation dot1q 21 *//Encapsulación subinterfaz g0/0/1.21*
R1(config-subif)#ip address 192.168.21.1 255.255.255.0 *//Asignación dirección ipv4 y mascara de subred*
R1(config-subif)#exit *//Salir de modo de configuración*

//Configurar la subinterfaz 802.1Q .23 en Gi0/0/1
R1(config)#interface gigabitEthernet 0/0/1.23 *//Crear subinterfaz g0/0/1.23*
R1(config-subif)#description LAN de Ingenieria *//Descripción g0/0/1.23*
R1(config-subif)#encapsulation dot1q 23 *//Encapsulación subinterfaz g0/0/1.23*
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 *//Asignación dirección ipv4 y mascara de subred*
R1(config-subif)#exit *//Salir de modo de configuración*

//Configurar la subinterfaz 802.1Q .99 en Gi0/0/1
R1(config)#interface gigabitEthernet 0/0/1.99 *//Crear subinterfaz g0/0/1.99*

R1(config-subif)#description LAN de Administracion *//Descripción g0/0/1.99*
R1(config-subif)#encapsulation dot1q 99 *//Encapsulación subinterfaz g0/0/1.99*
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 *//Asignación dirección ipv4 y mascara de subred*
R1(config-subif)#exit *//Salir de modo de configuración*

//Activar la interfaz Gi0/0/1
R1(config)#interface gigabitEthernet 0/0/1 *//Configurar interfaz*
R1(config-if)#no shutdown *//Comando para habilitar la interfaz*
R1(config-if)#exit *//Salir de modo de configuración*

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

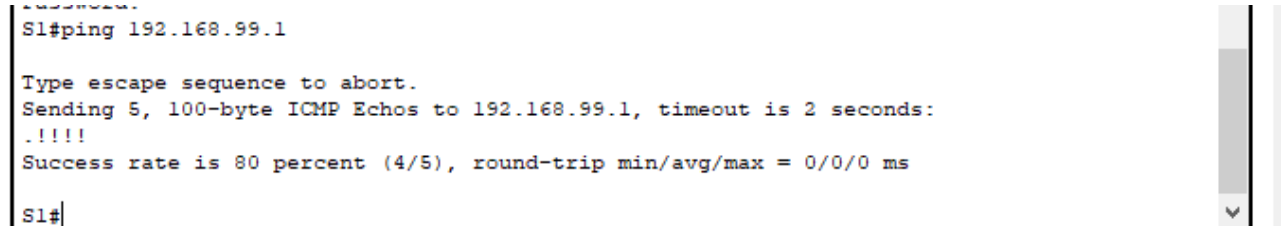
Tabla 15. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	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	R1, dirección VLAN 99	192.168.99.1	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 = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to

			192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

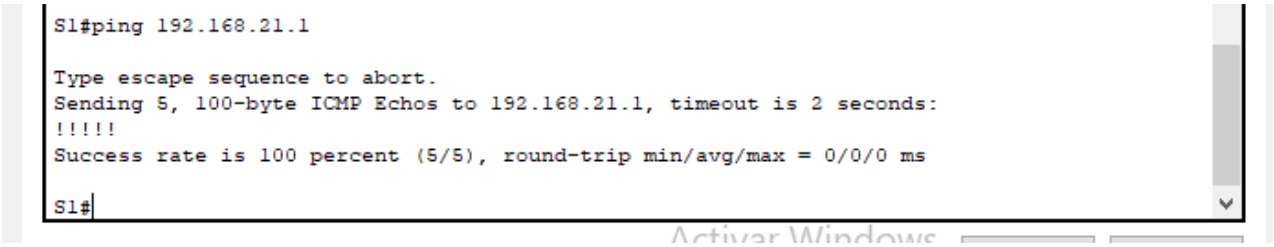
Fuente propia

Figura 14. Ping de S1 a R1 Vlan 99



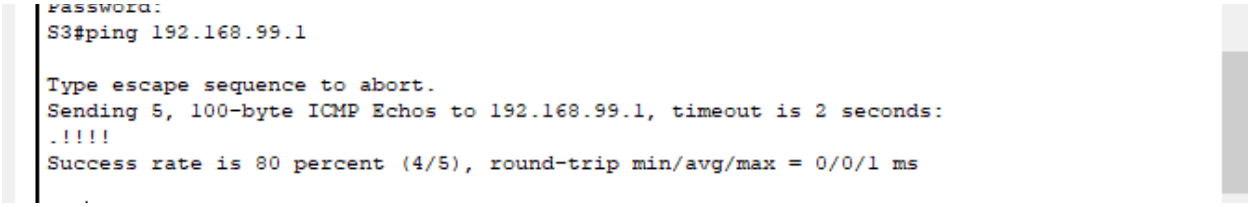
Fuente propia

Figura 15. Ping de S1 a R1 Vlan 21



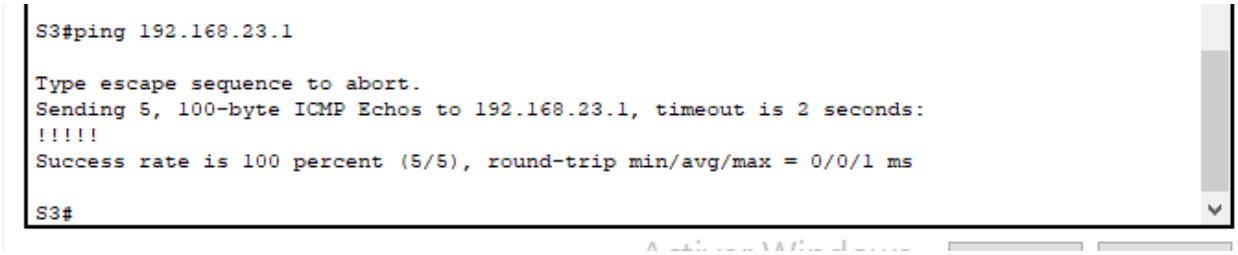
Fuente propia

Figura 16. Ping de S3 a R1 Vlan 99



Fuente propia

Figura 17. Ping de S3 a R1 Vlan 23



Fuente propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configurar OSPF en el R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Fuente propia

Router 1

R1>enable *//Acceso a modo EXEC privilegiado*
Password: // Ingreso contraseña
R1#configure terminal *//Ingreso a modo configuración*
R1(config)#router ospf 1 *//Configuración de OSPF*

//Anunciar las redes conectadas directamente
R1(config-router)#do show ip route c *//Comando para mostrar redes conectadas directamente*
C 172.16.1.0/30 is directly connected, Serial0/2/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/0/1.99

R1(config-router)#network 172.16.1.0 255.255.255.252 area 0 *//Red 172.16.1.0 conectada directamente*
R1(config-router)#network 192.168.21.0 255.255.255.0 area 0 *//Red 192.168.21.0 conectada directamente*

R1(config-router)#network 192.168.23.0 255.255.255.0 area 0 *//Red 192.168.23.0 conectada directamente*
R1(config-router)#network 192.168.99.0 255.255.255.0 area 0 *//Red 192.168.99.0 conectada directamente*

//Establecer todas las interfaces LAN como pasivas
R1(config-router)#passive-interface gigabitEthernet0/0/1.21 *//Activar interfaz g0/0/1.21 como pasiva*
R1(config-router)#passive-interface gigabitEthernet0/0/1.23 *//Activar interfaz g0/0/1.23 como pasiva*
R1(config-router)#passive-interface gigabitEthernet0/0/1.99 *//Activar interfaz g0/0/1.99 como pasiva*

//Desactive la sumarización automática
R1(config-router)#area 1 stub no-summary

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 17. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática	

Fuente propia

Router 2

R2>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso Contraseña*
R2#configure terminal *//Ingreso a modo configuración*
R2(config)#router ospf 1 *//Configuración de OSPF*

//Anunciar las redes conectadas directamente
R2(config-router)#do show ip route c *//Comando para mostrar redes conectadas directamente*
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/2/0
C 172.16.2.0/30 is directly connected, Serial0/2/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0/0

R2(config-router)#network 10.10.10.10 255.255.255.255 área 0 *//Red 10.10.10.10 conectada directamente*
R2(config-router)#network 172.16.1.0 255.255.255.252 área 0 *//Red 172.16.1.0 conectada directamente*
R2(config-router)#network 172.16.2.0 255.255.255.252 área 0 *//Red 172.16.2.0 conectada* directamente

//Establecer la interfaz LAN (loopback 0) como pasiva
R2(config-router)#passive-interface lo0

//Desactive la sumarización automática
R2(config-router)#area 1 stub no-summary

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 18. Configurar OSPFv3 en el R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Fuente propia

Router 3

R3>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso Contraseña*

R3#configure terminal *//Ingreso a modo configuración*
R3(config)#router ospf 1 *//Configuración de OSPF*

//Anunciar las redes conectadas directamente
R3(config-router)#do show ip route c *//Comando para mostrar redes conectadas directamente*
C 172.16.2.0/30 is directly connected, Serial0/2/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6

R3(config-router)#network 172.16.2.0 255.255.255.252 area 0 *//Red 172.16.2.0 conectada directamente*
R3(config-router)#network 192.168.4.0 255.255.255.0 area 0 *//Red 192.168.4.0 conectada directamente*
R3(config-router)#network 192.168.5.0 255.255.255.0 area 0 *//Red 192.168.5.0 conectada directamente*
R3(config-router)#network 192.168.6.0 255.255.255.0 area 0 *//Red 192.168.6.0 conectada directamente*

//Establecer todas las interfaces LAN como pasivas
R3(config-router)#passive-interface lo4 *//Establecer interfaz lo4 como pasiva*
R3(config-router)#passive-interface lo5 *//Establecer interfaz lo5 como pasiva*
R3(config-router)#passive-interface lo6 *//Establecer interfaz lo6 como pasiva*

//Desactive la sumarización automática
R3(config-router)#area 1 stub no-summary

Paso 4: Verificar la información de OSPF

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

Tabla 19. Verificar la información de 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?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf

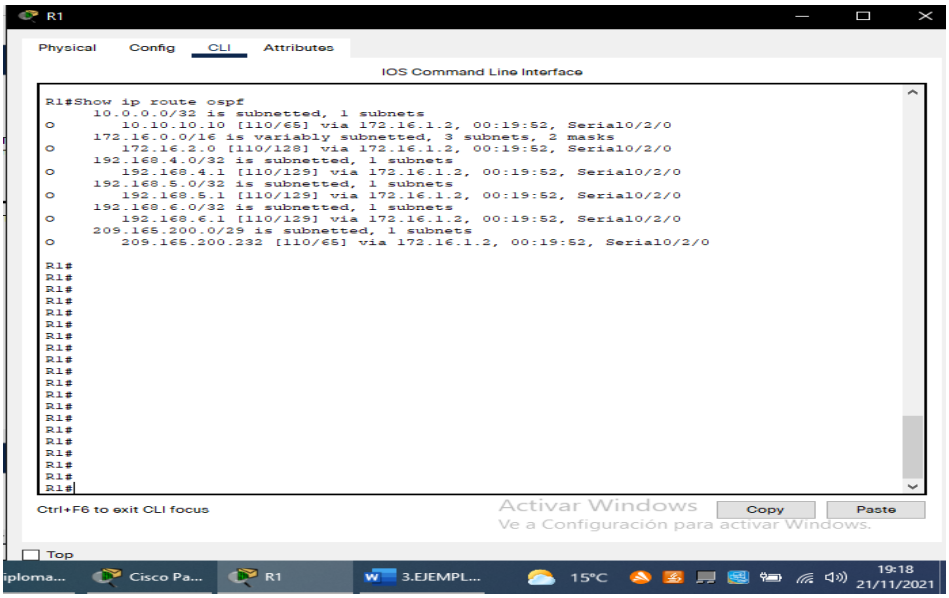
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf database

Fuente propia

Figura 18. Verificación comando Show ip protocols

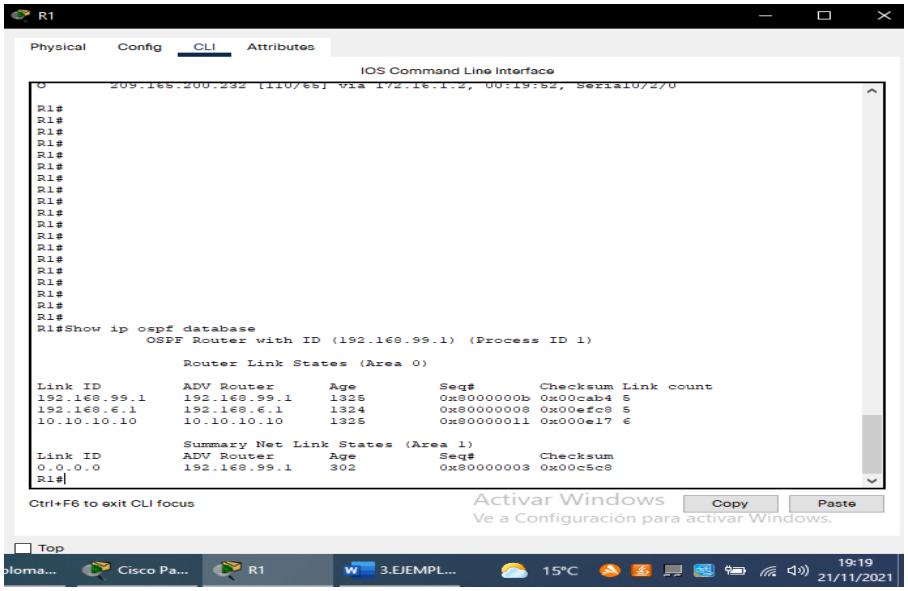
Fuente propia

Figura 19. Verificación comando Show ip route ospf



Fuente propia

Figura 20. Verificación comando Show ip ospf database



Fuente propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 20. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente propia

Router 1

R1#configure t *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.

//Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

//Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

//Crear un pool de DHCP para la VLAN 21.
R1(config)#ip dhcp pool ACCT *Crear un pool ACCT*
R1(dhcp-config)#dns-server 10.10.10.10 *//Asignación servidor DNS*
R1(dhcp-config)#domain-name ccna-sa.com *//Creación dominio ccna-sa.com*
R1(dhcp-config)#default-router 192.168.21.1 *//Asignación router por defecto 192.168.21.1*
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 *//Asignación red 192.168.21.0/24*
R1(dhcp-config)#exit *//Salir de modo de configuración*

//Crear un pool de DHCP para la VLAN 23
R1(config)#ip dhcp pool ENGNR *//Crear un pool* ENGNR
R1(dhcp-config)#dns-server 10.10.10.10 *//Asignación servidor DNS*
R1(dhcp-config)#domain-name ccna-sa.com *//Creación dominio ccna-sa.com*
R1(dhcp-config)#default-router 192.168.23.1 *//Asignación router por defecto 192.168.23.1*
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 *//Asignación red 192.168.23.0/24*
R1(dhcp-config)#exit *//Salir de modo de configuración*

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

La configuración del R2 incluye las siguientes tareas:

Tabla 21. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**

Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	

Fuente propia

Router 2

R2>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso Contraseña*
R2#configure terminal *//Ingreso a modo configuración*
Enter configuration commands, one per line. End with CNTL/Z.

//Crear una base de datos local con una cuenta de usuario
R2(config)#user webuser privilege 15 secret cisco 12345
//Habilitar el servicio del servidor HTTP (Comando no soportado en el simulador)
R2(config)#ip http server
R2(config)#ip http authentication local
//Crear una NAT estática al servidor web.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233

//Asignar la interfaz interna y externa para la NAT estática
R2(config)#interface gig0/0/0 *//Configurar interfaz gig0/0/0*
R2(config-if)#ip nat outside *//Asignación como interfaz externa*
R2(config-if)#exit
R2(config)#interface serial0/2/0 *//Configurar interfaz gig0/0/0*
R2(config-if)#ip nat inside *//Asignación como interfaz interna*
R2(config-if)#exit
R2(config)#interface serial0/2/1 *//Configurar interfaz serial0/2/1*
R2(config-if)#ip nat inside *//Asignación como interfaz interna*
R2(config-if)#exit *//Salir de modo de configuración*

//Configurar la NAT dinámica dentro de una ACL privada
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 *//Creación primera lista de acceso*
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 *//Creación segunda de acceso*
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 *//Creación tercera lista de acceso*

R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 *//Creación cuarta lista de acceso*
R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 *//Creación quinta lista de acceso*

//Defina el pool de direcciones IP públicas utilizables.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

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

Paso 3: Verificar el protocolo DHCP y la NAT estática

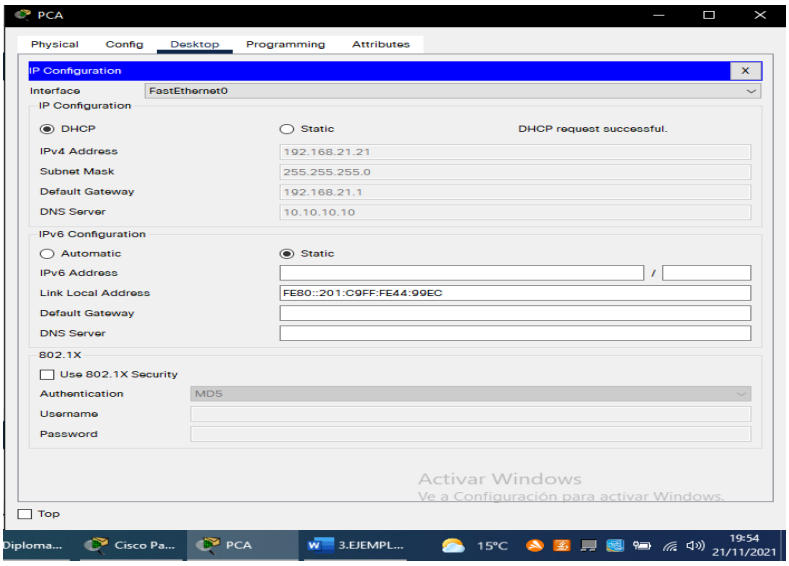
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 22. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	OK
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	OK
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	OK
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

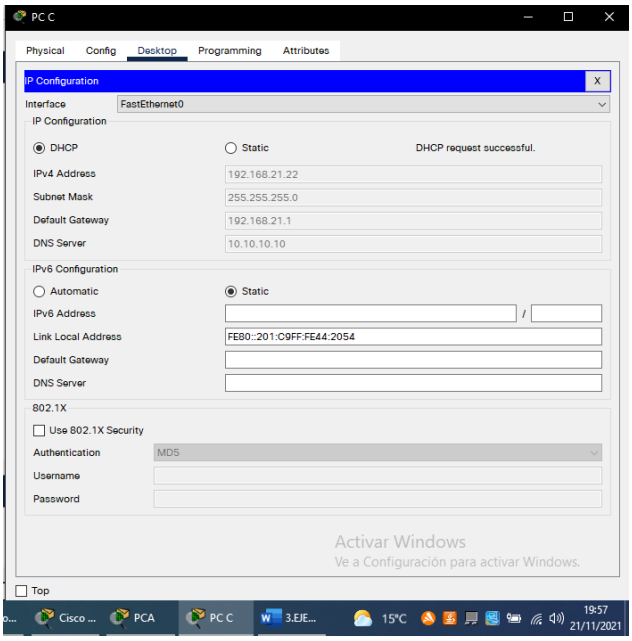
Fuente propia

Figura 21. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



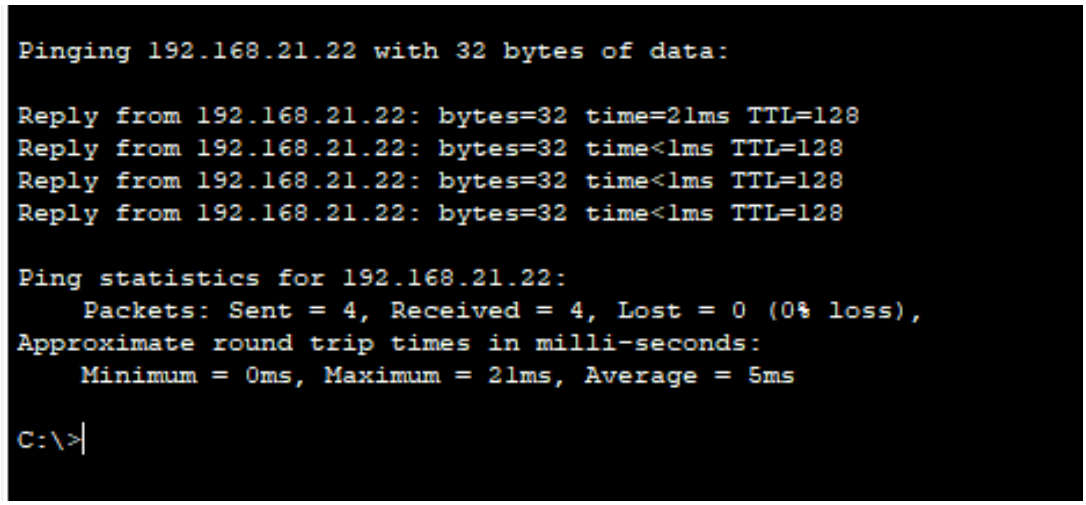
Fuente propia

Figura 22. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente propia

Figura 23. Verificar que la PC-A pueda hacer ping a la PC-C



Fuente propia

Tabla 23. Configurar NTP

Parte 6: Configurar NTP

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Fuente propia

Router 2

//Ajuste la fecha y hora en R2.
R2#clock set 09:00:00 5 Mar 2016

R2#configure terminal *//Ingreso a modo configuración*
//Configure R2 como un maestro NTP.
R2(config)#ntp master 5

Router 1

R1>enable *//Acceso a modo EXEC privilegiado*
Password: *//Ingreso contraseña*
R1#configure terminal *//Ingreso a modo configuración*
//Configurar R1 como un cliente NTP.
R1(config)#ntp server 172.16.1.2

//Configure R1 para actualizaciones de calendario periódicas con hora NTP.
R1(config)#ntp update-calendar
R1(config)#exit *//Salir modo de configuración*

//Verifique la configuración de NTP en R1.

R1#show ntp status
Clock is synchronized, stratum 6, reference is 172.16.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA6035A9.000001CD (9:4:41.461 UTC Sat Mar 5 2016)
clock offset is 0.00 msec, root delay is 2.00 msec
root dispersion is 10.23 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system

poll interval is 4, last update was 2 sec ago.

R1#show ntp associations

address ref clock st when poll reach delay offset disp
*~172.16.1.2 127.127.1.1 5 14 16 377 11.00 3.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1#show clock
9:7:32.86 UTC Sat Mar 5 2016

Figura 24. Comandos para Verificar la configuración de NTP en R1

```
R1#show ntp status
Clock is synchronized, stratum 6, reference is 172.16.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA6035A9.000001CD (9:4:41.461 UTC Sat Mar 5 2016)
clock offset is 0.00 msec, root delay is 2.00 msec
root dispersion is 10.23 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 2 sec ago.
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
*~172.16.1.2    127.127.1.1     5    14       16      377    11.00          3.00
0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#show clock
9:7:32.86 UTC Sat Mar 5 2016
R1#
```

Fuente propia

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

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

Tabla 24. Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Fuente propia

Router 2

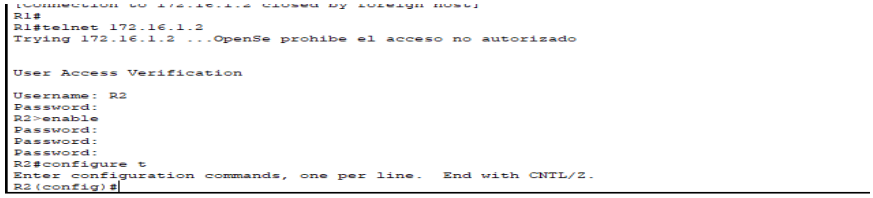
R2#configure terminal *//Ingreso a modo configuración*

//Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2
R2(config)#ip access-list standard ADMIN-MGT *//Configuración lista estandar ADMIN-MGT*
R2(config-std-nacl)#permit host 172.16.1.1 *//Solo se permite acceso a 172.16.1.1*
R2(config-std-nacl)#exit *//Salir modo de configuración*

//Aplicar la ACL con nombre a las líneas VTY
R2(config)#line vty 0 4 *//configuración linea telnet*
R2(config-line)#access-class ADMIN-MGT in *//Aplicación ACL con nombre a las líneas VTY*
R2(config-line)#exit *//Salir modo de configuración*

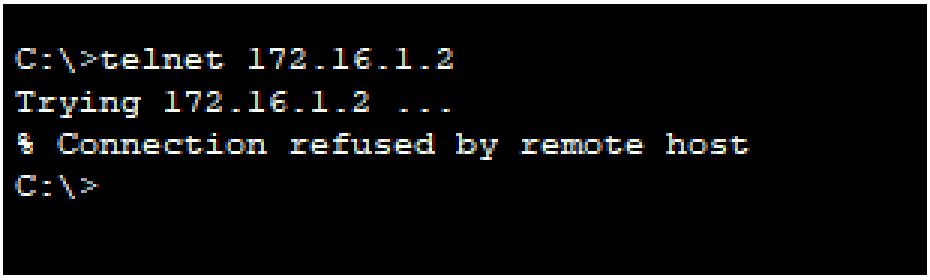
//Permitir acceso por Telnet a las líneas de VTY
R2(config)#line vty 0 4 *//configuración linea telnet*
R2(config-line)#transport input telnet *//Permiso acceso por telnet*
R2(config-line)#exit *//Salir modo de configuración*
//Verificar que la ACL funcione como se espera

Figura 25. Verificación acceso Telnet desde R1



Fuente propia

Figura 26. Verificación acceso telnet de PC-A a R2



Fuente propia

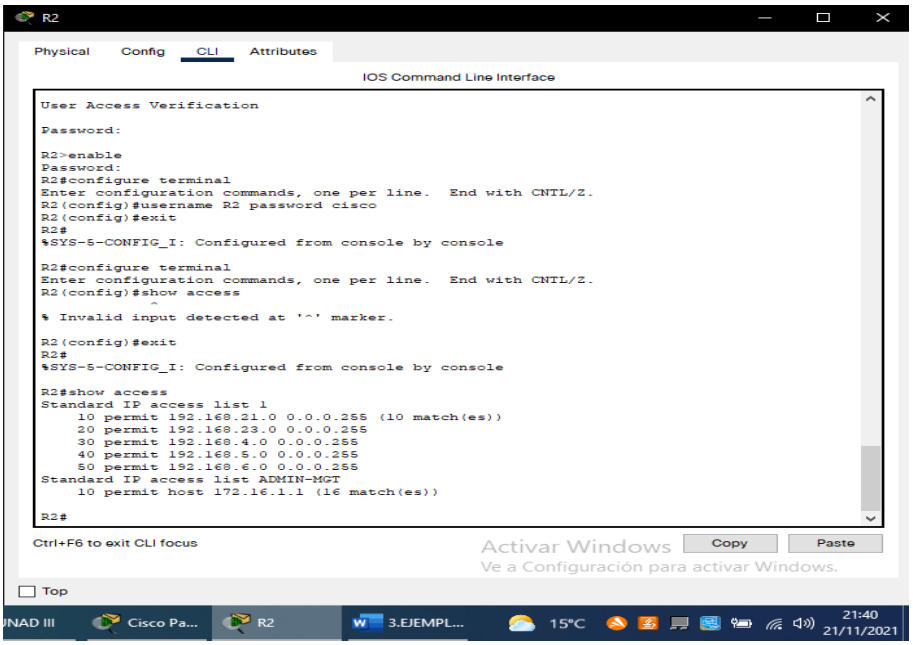
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 25. Introducir el comando de CLI

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
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface gig0/0/0 | include access list Outgoing access list is not set Inbound access list is not set R2#show ip interface gig0/0/0 | include access Outgoing access list is not set Inbound access list is not set IP access violation accounting is disabled
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	**R2#**clear ip nat translation *

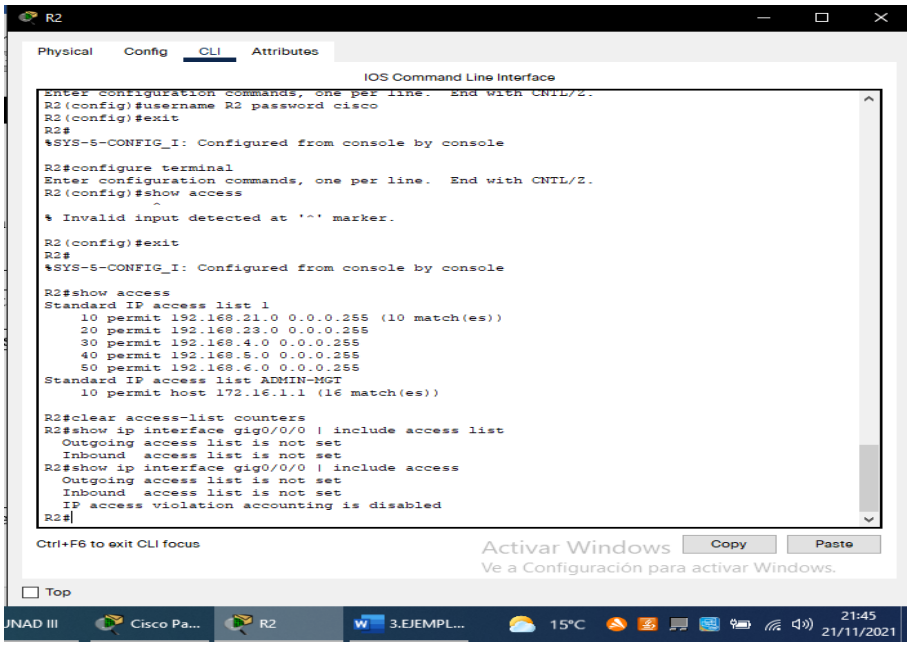
Fuente propia

Figura 27. Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció



Fuente propia

Figura 28. Restablecer los contadores de una lista de acceso



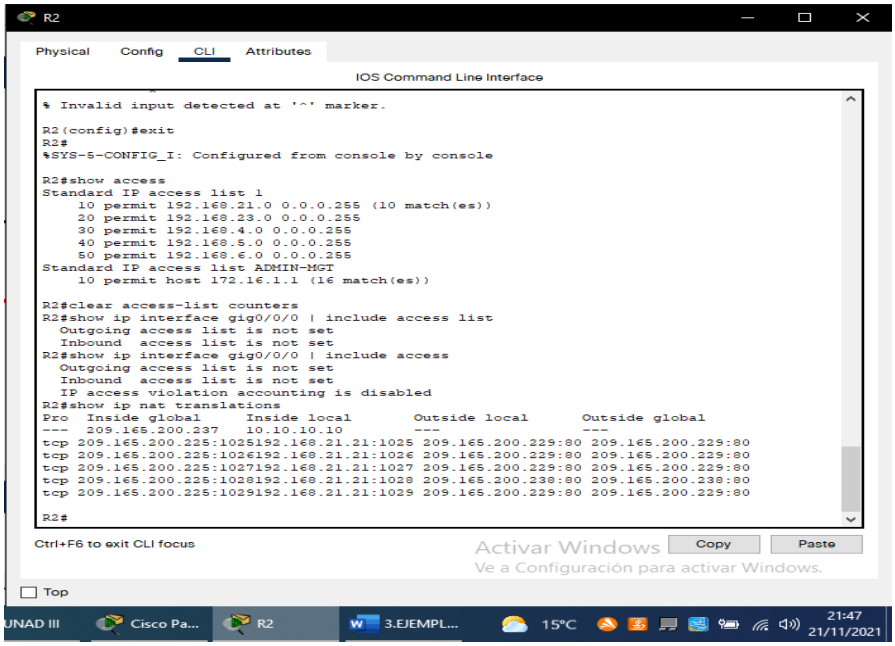
Fuente propia

¿Con qué comando se muestran las traducciones NAT?

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.225:1025192.168.21.21:1025 209.165.200.229:80
209.165.200.229:80
tcp 209.165.200.225:1026192.168.21.21:1026 209.165.200.229:80
209.165.200.229:80
tcp 209.165.200.225:1027192.168.21.21:1027 209.165.200.229:80
209.165.200.229:80
tcp 209.165.200.225:1028192.168.21.21:1028 209.165.200.238:80
209.165.200.238:80
tcp 209.165.200.225:1029192.168.21.21:1029 209.165.200.229:80

209.165.200.229:80

Figura 29. Comando para mostrar traducciones NAT



Fuente propia

CONCLUSIONES

El uso de herramientas de simulación permitió realizar un análisis de todos los conocimientos adquiridos en el diplomado CCNA, usando protocolos para la configuración básica de routers y switchs.

Se realizo la topología propuesta del escenario 1, verificando la conectividad entre cada uno de los equipos por medio de comando ping, e ingreso por conexión SSH.

Por medio de este trabajo se observó la importancia del esquema de direccionamiento de red, como parte inicial y fundamental para el correcto desarrollo del escenario 1.

Comprendí el uso de las vlans, como método para la creación de varias redes independientes dentro de una misma red, ofreciendo a los usuarios una mejor organización de red por áreas.

Una de las partes más importantes de una red es su seguridad y con el uso de protocolos como DHCP para asignación dinámica de direcciones IP, obtenemos esta cualidad en nuestra red.

BIBLIOGRAFIA

[1] 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.

[2] GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

[3] 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.

[4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

[5] 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.

[6] 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.

[7] MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

[8].“Enrutamiento y sus características” Redes de computadoras. Recuperado de https://sites.google.com/site/redesdecomputadorashamed/unidad-3-capas-inferiores-del-modelo-osi-y-tcp-ip/3-1-capa-de-red/3-1-3-enrutamiento-y-sus-caracteristicas

[9]. (2013) “Concepto de red” Que es una red. Recuperado de. https://concepto.de/red-2/

[10]. (2021) “Comando ping”. Wikipedia. Recuperado de https://es.wikipedia.org/wiki/Ping