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

CARLOS ALBERTO IBAÑEZ PAREDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
EL CARMEN DE BOLIVAR, BOLIVAR.

2021

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

CARLOS ALBERTO IBAÑEZ PAREDES

DIRECTOR:
NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
EL CARMEN DE BOLIVAR, BOLIVAR.
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

EL CARMEN DE BOLIVAR, noviembre de 2021

AGRADECIMIENTOS

Al creador principalmente por la oportunidad de seguir adelante cada día con todas fuerzas que él me brinda, mis primeros agradecimientos. A mis padres y mis hijos quienes me han apoyado en cada instante de mi vida y han sido mi sostén, a mis hermanos quienes me aconsejan y me guían. A todos los compañeros y tutores, en particular al ingeniero Raul Bareño Gutierrez, quienes me ayudaron en cada etapa y los que aún siguen en la batalla igual que yo, mis más sinceros agradecimientos a todos los que me dejaron buenas enseñanzas y experiencias.

CONTENIDO

AGRADECIMIENTOS 4
LISTA DE TABLAS....7
LISTA DE FIGURAS....8
GLOSARIO....9
RESUMEN 10
ABSTRACT 10
INTRODUCCION....11
DESARROLLO....12
Escenario 1 12
Parte 1: Construcción de la red....12
Parte 2: Desarrollo del esquema de direccionamiento IP 13
Parte 3: Configuración de aspectos básicos y ajustes básicos de red....13
Paso 1. Configuraciones básicas de S1 15
Paso 2: Configuración de los equipos y comprobación de conectividad. 16
Escenario 2 20
Parte 1. Inicializar dispositivos 21
Paso 1. Inicializar y volver a cargar los routers y los switchs. 21
Parte 2. Configurar los parámetros básicos de los dispositivos. 21
Paso 1. Configurar la computadora de Internet 21
Paso 2. Configuración básica R1....22
Paso 3. Configuración básica R2....23
Paso 4. Configuración básica R3....24
Paso 5. Configuración básica S1....25
Paso 6. Configuración básica S3....26
Paso 7 verificar la conectividad de la red....27
Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN 28
Paso 1. Configurar la seguridad del switch, las VLAN y el routing entre VLAN de S1 28
Paso 2. Configurar la seguridad del switch, las VLAN y el routing entre VLAN de S3 29
Paso 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN de R1 30
Paso 4 verificar la conectividad de la red....31
Parte 4. Configurar el protocolo de routing dinámico OSPF 32
Paso 1. Configurar OSPF en el R1....32

Paso 2. Configurar OSPF en el R2 33
Paso 3. Configurar OSPFv3 en el R2 33
Paso 4. Configurar OSPFv3 en el R3 34
R3(config)#ipv6 router ospf 74 34
R3(config)#interface s0/2/1 34
R3(config-if)#ipv6 ospf 74 area 0 34
R3(config)#ipv6 router ospf 74 34
R3(config-rtr)#passive-interface lo 4 34
R3(config-rtr)#passive-interface lo 5 34
R3(config-rtr)#passive-interface lo 6 34
Desactive la sumarización automática 34
Paso 4. Verificar la información de OSPF 34
Parte 5. Implementar DHCP y NAT para IPv4 35
Paso 1. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 35
Paso 2. Configurar la NAT estática y dinámica en el R2 36
Paso 3. Verificar el protocolo DHCP y la NAT estática 37
Parte 6. Configurar NTP 39
Parte 7. Configurar y verificar las listas de control de acceso (ACL) 40
Paso 1. Restringir el acceso a las líneas VTY en el R2 40
Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 41
CONCLUSIONES 42
BIBLIOGRAFIA 43

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento ……13
Tabla 2. Tabla de configuración PC-A ……16
Tabla 3. Tabla de configuración PC-B ……17
Tabla 4. Comandos de inicialización de routers y switches ……21
Tabla 5. Configuración del servidor de internet ……21

LISTA DE FIGURAS

Figura 1. Topología de red escenario 1 ……12
Figura 2. Ip configuración PC-A ……16
Figura 3. Ipconfig /all PC-A ……17
Figura 4. Ip configuración PC-B ……17
Figura 5. Ipconfig /all PC-B ……18
Figura 6. PING desde PC-A a PC-B ……18
Figura 7. PING desde PC-B a PC-A ……19
Figura 8. Topología de red escenario 2 ……20
Figura 9. Configuración del servidor de internet ……21
Figura 10. Ping desde R1 a R2 ……27
Figura 11. Ping desde R2 a R3 ……27
Figura 12. Ping desde PC de internet a Gateway predeterminado ……27
Figura 13. Ping de S1 a R1 vlan 99 ……31
Figura 14. Ping de S3 a R1 vlan 99 ……31
Figura 15. Ping de S1 a R1 vlan 21 ……31
Figura 16. Ping de S3 a R1 vlan 23 ……32
Figura 17. Comando show ip protocols ……34
Figura 18. Comando show ip route ospf ……35
Figura 19. Comando show running-config (show run) ……35
Figura 20. DHCP PC-A ……38
Figura 21. DHCP PC-C ……38
Figura 22. Ping de PC-A a PC-C ……38
Figura 23. Acceso a http://209.165.200.238 ……39
Figura 24. Show clock ……39
Figura 25. Telnet 172.16.1.2 ……40
Figura 26. Comando show access-list ……41
Figura 27. Show ip nat translations ……41

GLOSARIO

Ajustes: Acomodar los dispositivos de red de acuerdo a los requerimientos.

Comando: Orden que se le da a un programa que actúa como intérprete del mismo.

Contraseña: Una palabra formada por caracteres que sirve a uno o más usuarios para acceder a un determinado recurso.

Conexión: Unión que se establece entre dos o más cosas (Aparatos, sistemas, lugares, etc…)

Consola: Es una estación de trabajo convenientemente configurada para visualizar la información recogida por los agentes (Programas que recogen información).

DHCP: (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red de forma dinámica.

Dominio: Nombre único que identifica a un sitio en particular.

Gateway: O «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP.

Interfaz: Zona de comunicación o acción de un sistema sobre otro.

Ospf: **Open Shortest Path First** (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP)

Router: es un dispositivo que ofrece una conexión, que normalmente está conectado a internet y que envía información a dispositivos personales, como ordenadores, teléfonos o tablets.

Switch: Switch es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.

RESUMEN

Se van a desarrollar dos escenarios de redes conmutadas, aplicando tecnología CISCO, basados en el enrutamiento de paquetes en dos redes de hasta un máximo 150 equipos en el primero y comunicación por protocolo OSPF, seguridad en dispositivos y asignación de ip DCHP, conectadas mediante dispositivos de redes configurados usando comandos tales como enable, banner motd, no ip domain-lookup, entre otros. La base del proyecto es poder realizar comunicación, optimizando recursos y minimizando gastos, siguiendo los lineamientos del diplomado CISCO CCNA.

Los dos escenarios exigen configuración de equipos electrónicos mediante puertos de consola y comandos CLI, desde la configuración básica como asignar nombres de dispositivos y direcciones ip, hasta creación de vlan y enrutamiento entre las mismas, sub interfaces, asignación de direcciones con DHCP que será configurado en un router lo cual aumentara las capacidades de este y reducirá costos en equipos servidores. Se crearán listas de control de acceso (ACL), que nos permitirán controlar el acceso creando tablas de permitidos y negados. El resultado final son dos redes que tienen comunicación óptima y de calidad más seguridad.

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

ABSTRACT

Two scenarios of switched networks will be developed, applying CISCO technology, based on packet routing in two networks of up to a maximum of 150 computers in the first and communication by OSPF protocol, security in devices and DCHP ip assignment, connected by network devices configured using commands such as enable, banner motd, no ip domain-lookup, among others. The basic of the project is to be able to carry out communication, optimizing resources and minimizing expenses, following the guidelines of the CISCO CCNA graduate.

Both scenarios require configuration of electronic equipment using console ports and cli commands from basic settings such as assigning device names and ip addresses, until creation of vlan and routing between them, sub interfaces, assignment of addresses with DHCP that will be configured in a router which will increase the capabilities of this and reduce costs in server equipment. The end result is two networks that have optimal communication and quality plus security.

Keywords: CISCO, CCNA, Switching, Routing, Networking, Electronics.

INTRODUCCION

El diplomado de profundización CISCO tiene como objetivo principal desarrollar en los estudiantes competencias para configurar y administrar dispositivos de Networking, orientados al diseño y administración de redes. Abordando temas como configuración de sistemas operativos de red, protocolos de comunicación, mecanismos de acceso al medio y características de la capa de red, capa de transporte, asignación de direcciones IP y subneting.

En cada paso y actividad desarrollada se irán adquiriendo nuevas competencias y reforzando los existentes, apoyados en herramientas como el escenario de simulación Cisco Packet Tracer que permite realizar conexiones y configuraciones que refuerzan el conocimiento y las habilidades. En donde se desarrollan dos problemas de red. Es necesario implementar las configuraciones básicas y de seguridad de cada dispositivo de red, como pc, switch, routers, servidores, y cableado. Todo lo necesario para realizar una red con conectividad y comunicación.

Para las configuraciones de dispositivos de capa dos y tres se usaran los métodos de consola y cli, se aplicará protocolo ospf que es un protocolo de enrutamiento dinámico interior, se crearán vlan que son reden lógicas creadas dentro de una misma red física, lo cual nos permite aprovechar de forma exponencial los recursos de infraestructura, y traducción de direcciones NAT. Aplicando seguridad además con uso de contraseñas y listas de control de acceso (ACL). Se logrará sacarle el máximo provecho a cada dispositivo y protocolo para aumentar la calidad de la conectividad y comunicación así como la seguridad.

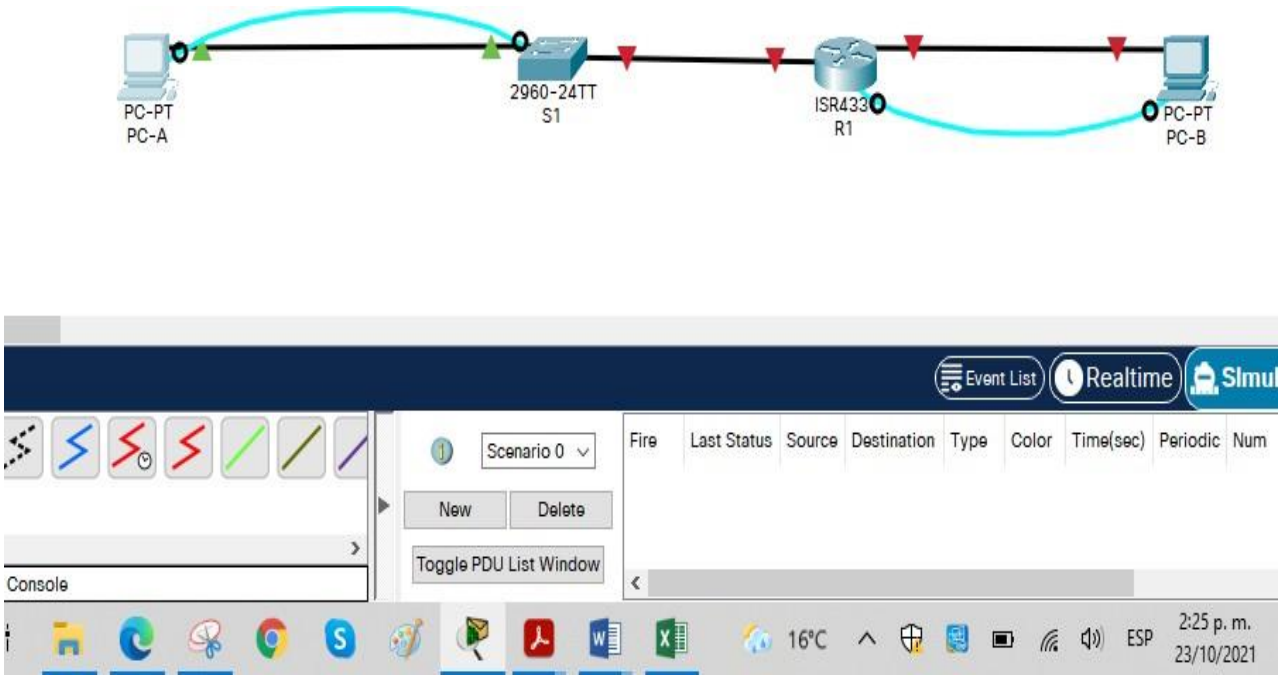
DESARROLLO

Escenario 1

Parte 1: Construcción de la red.

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

Figura 1. Topología de red escenario 1.



Fuente propia.

Parte 2: Desarrollo del esquema de direccionamiento IP.

Tabla 1. Tabla de direccionamiento.

Ítem	Requerimiento
Dirección de Red	192.168.73.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.73.1
R1 G0/0/0	192.168.73.129
S1 SVI	192.168.73.2
PC-A	192.168.73.126
PC-B	192.168.73.190

Parte 3: Configuración de aspectos básicos y ajustes básicos de red.
R1

Comando	Descripción del comando
Router>enable	Ingresar al modo administrador
Router#config terminal	Ingresar al modo de configuración global
Router(config)#no ip domain-lookup	Desactivar la traducción de nombres a dirección de dispositivos
Router(config)#hostname R1	Asignar nombre al dispositivo como R1
R1(config)#ip domain-name ccna-lab.com	Asignar el nombre ccna-lab.com al dominio
R1(config)#enable secret ciscoenpass	Asignar contraseña cifrada ciscoenpass para acceder al modo privilegiado
R1(config)#line console 0	Acceder a configuración de una línea de consola del router
R1(config-line)#password ciscoconpass	Crear la contraseña de acceso ciscoconpass a la línea de consola 0
R1(config-line)#login	Crear la solicitud de autenticación para

	la contraseña creada
R1(config-line)#exit	Salir de configuración línea cero y regresar a configuración global
R1(config)#security password min-length 10	Asignar el largo minimo de 10 caracteres para los passwords
R1(config)#username admin password admin1pass	Se crea el usuario admin y se le asigna la contraseña admin1pass
R1(config)#line vty 0 4	Se accede a linea vty del router
R1(config-line)#password ciscocisco	Se le asigna la contraseña ciscocisco minimo 10 caracteres
R1(config-line)#login local	Se configura autenticación local
R1(config-line)#transport input ssh	Se configura para que solo permita conexión ssh
R1(config-line)#exit	Salir de configuración de línea vty
R1(config)#service password-encryption	Se cifran las contraseñas de texto no cifrado
R1(config)#banner motd #EL ACCESO NO AUTORIZADO ESTA PROHIBIDO#	Se crea un mensaje de aviso al momento del acceso al router
R1(config)#interface g0/0/0	Ingresa a interfaz g0/0/0 para configurarla
R1(config-if)#ip address 192.168.73.129 255.255.255.192	Se asigna dirección ip y mascara de subred a la interfaz g0/0/0
R1(config-if)#description ESTA ES LA INTERFAZ DE LA LAN 2	Se le da una descripción a la interfaz g0/0/0
R1(config-if)#no shutdown	Se activa la interfaz g0/0/0
R1(config-if)#exit	Salir de la configuración de la interfaz g0/0/0
R1(config)#interface g0/0/1	Ingresa a interfaz g0/0/1 para configurarla
R1(config-if)#ip address 192.168.73.1 255.255.255.128	Se asigna dirección ip y mascara de subred a la interfaz g0/0/1
R1(config-if)#description ESTA ES LA INTERFAZ DE LA LAN 1	Se le da una descripción a la interfaz g0/0/1
R1(config-if)#no shutdown	Se activa la interfaz g0/0/1
R1(config-if)#exit	Salir de la configuración de la interfaz g0/0/1
R1(config)#ip domain name ccna-lab.com	Se le asigna el nombre ccna-lab.com al dominio
R1(config)#crypto key generate rsa	Se genera una clave de cifrado de 1024 bits
R1(config)#exit	Se sale del modo de configuración global
R1#wr	Se guardan las configuraciones del dispositivo

Paso 1. Configuraciones básicas de S1

Comando	Descripción del comando
Switch>enable	Ingresar al modo administrador
Switch #config terminal	Ingresar al modo de configuración global
Switch (config)#no ip domain-lookup	Desactivar la traducción de nombres a dirección de dispositivos
Switch (config)#hostname S1	Asignar nombre al dispositivo como S1
S1(config)#ip domain-name ccna-lab.com	Asignar el nombre ccna-lab.com al dominio
S1(config)#enable secret ciscoenpass	Asignar contraseña cifrada ciscoenpass para acceder al modo privilegiado
S1(config)#line console 0	Acceder a configuración de una línea de consola del router
S1(config-line)#password ciscoconpass	Crear la contraseña de acceso ciscoconpass a la línea de consola 0
S1(config-line)#login	Crear la solicitud de autenticación para la contraseña creada
S1(config-line)#exit	Salir de configuración línea cero y regresar a configuración global
S1(config)#username admin password admin1pass	Se crea el usuario admin y se le asigna la contraseña admin1pass
S1(config)#line vty 0 15	Se accede a linea vty del switch
S1(config-line)#password ciscocisco	Se le asigna la contraseña ciscocisco
S1(config-line)#login local	Se configura autenticación local
S1(config-line)#transport input ssh	Se configura para que solo permita conexión ssh
S1(config-line)#exit	Salir de configuración de línea vty
S1(config)#service password-encryption	Se cifran las contraseñas de texto no cifrado
S1 (config)#banner motd #EL ACCESO NO AUTORIZADO ESTA PROHIBIDO#	Se crea un mensaje de aviso al momento del acceso al router
S1 (config)#ip domain name ccna-lab.com	Se le asigna el nombre ccna-lab.com al dominio
S1 (config)#crypto key generate rsa	Se genera una clave de cifrado de 1024 bits
S1 (config)#interface vlan 1	Ingresa a interfaz vlan 1 para configurarla

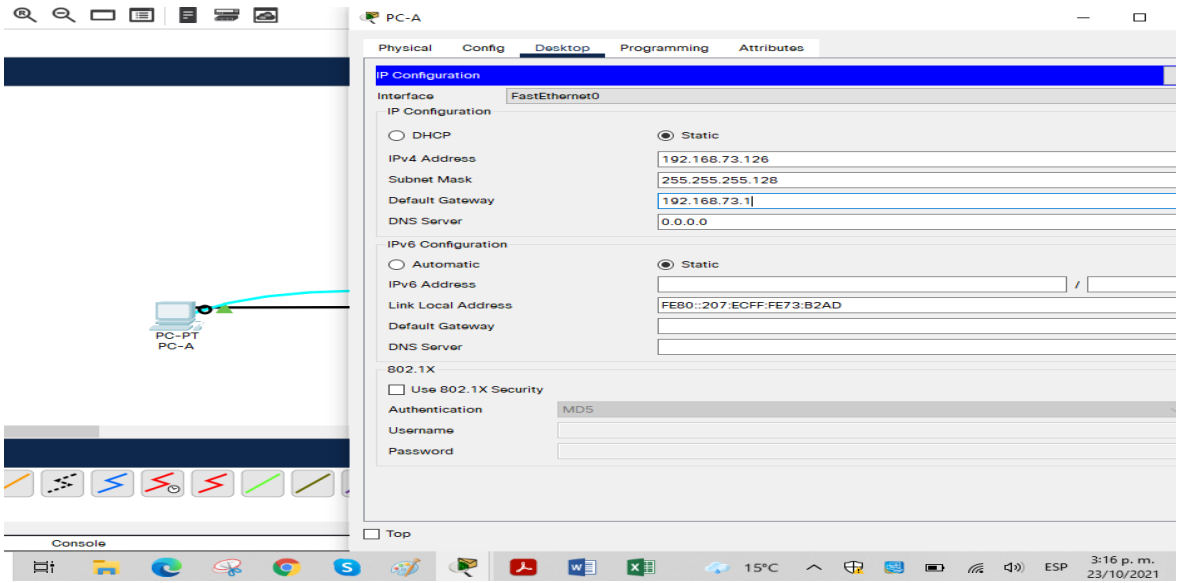
S1 (config-if)#ip address 192.168.73.2 255.255.255.128	Se asigna dirección ip y mascara de subred a la interfaz vlan 1
S1 (config-if)#no shutdown	Se activa la interfaz vlan 1
S1 (config-if)#exit	Salir de la configuración de la interfaz vlan 1
S1 (config)#ip default-gateway 192.168.73.1	Se asigna Gateway por defecto a la vlan 1
S1 (config)#exit	Se sale del modo de configuración global
S1#wr	Se guardan las configuraciones del dispositivo

Paso 2: Configuración de los equipos y comprobación de conectividad.

Tabla 2. Tabla de configuración PC-A

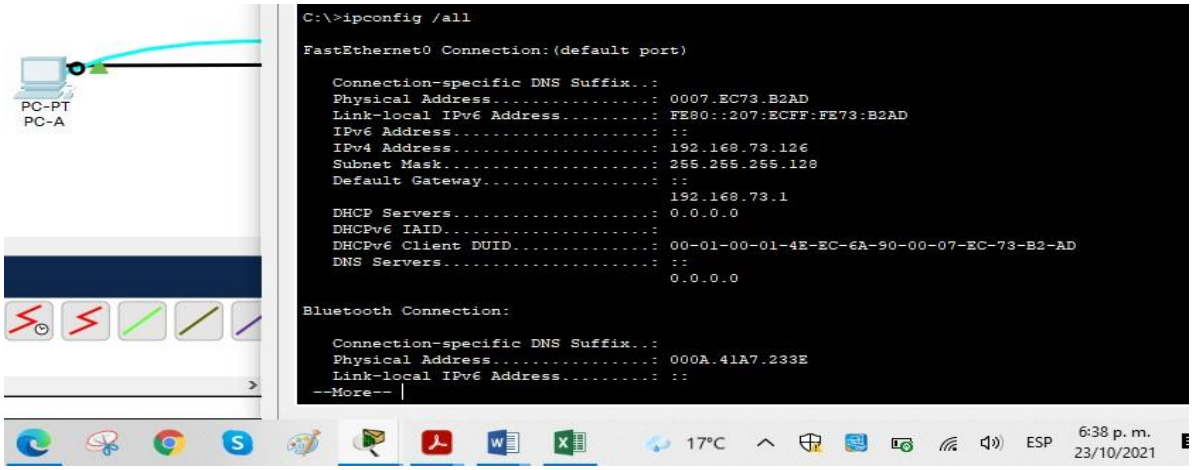
PC-A Network Configuration	
Descripción	Computadora A
Dirección física	0007.EC73.B2AD
Dirección IP	192.168.73.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.73.1

Figura 2. Ip Configuración PC-A



Fuente propia.

Figura 3. Ipconfig /all PC-A



Fuente propia.

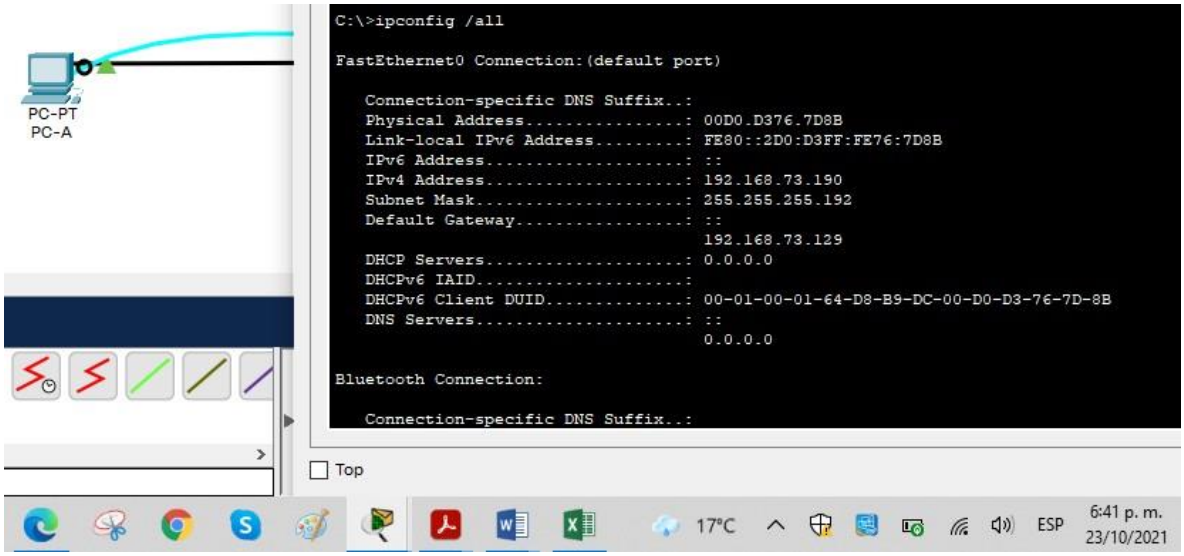
Tabla 3. Tabla de configuración PC-B

PC-B Network Configuration	
Descripción	Computadora B
Dirección física	00D0.D376.7D8B
Dirección IP	192.168.73.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.73.129

Figura 4. Ip configuración PC-B

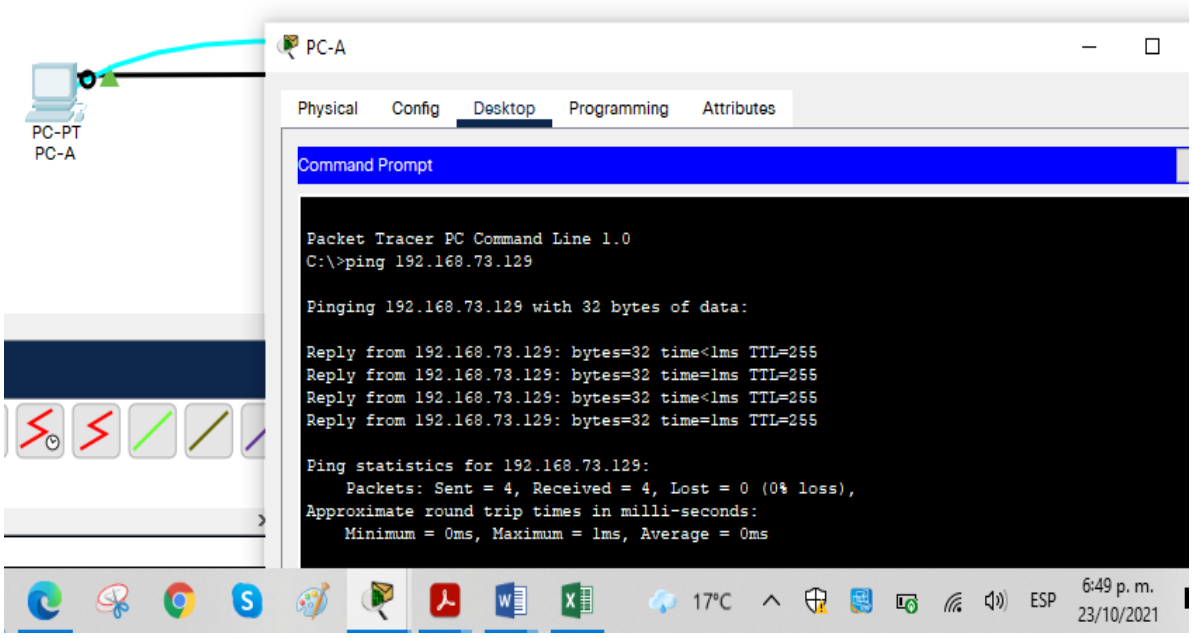
Fuente propia.

Figura 5. Ipconfig /all PC-B



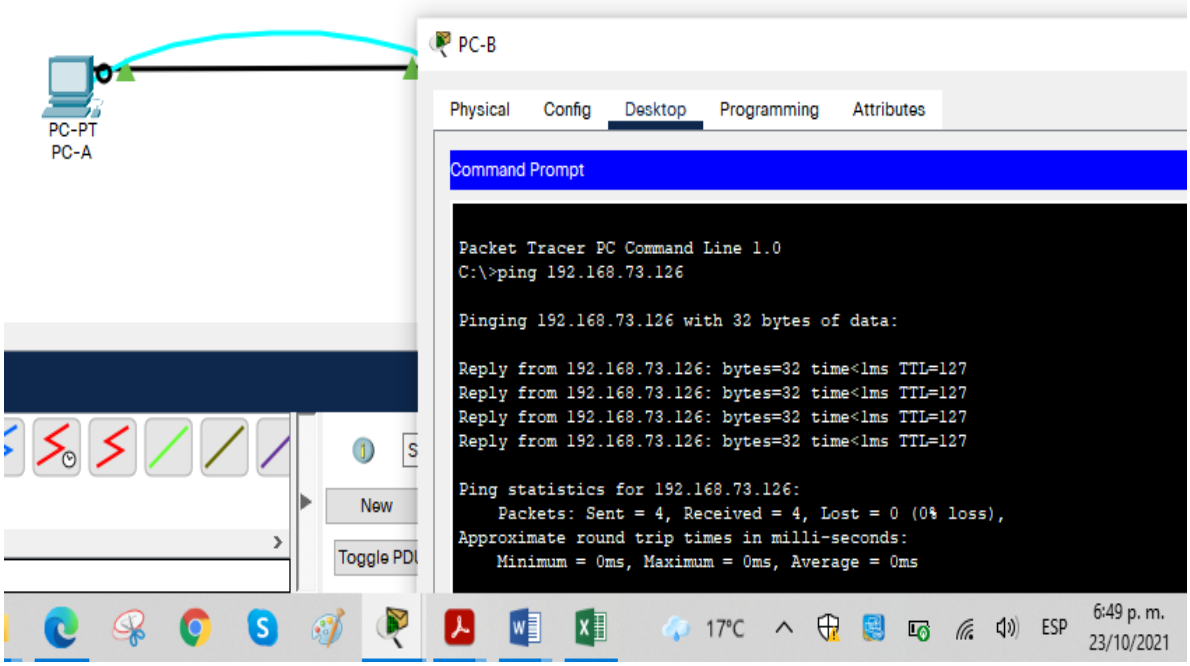
Fuente propia.

Figura 6. PING desde PC-A a PC-B



Fuente propia.

Figura 7. PING desde PC-B a PC-A

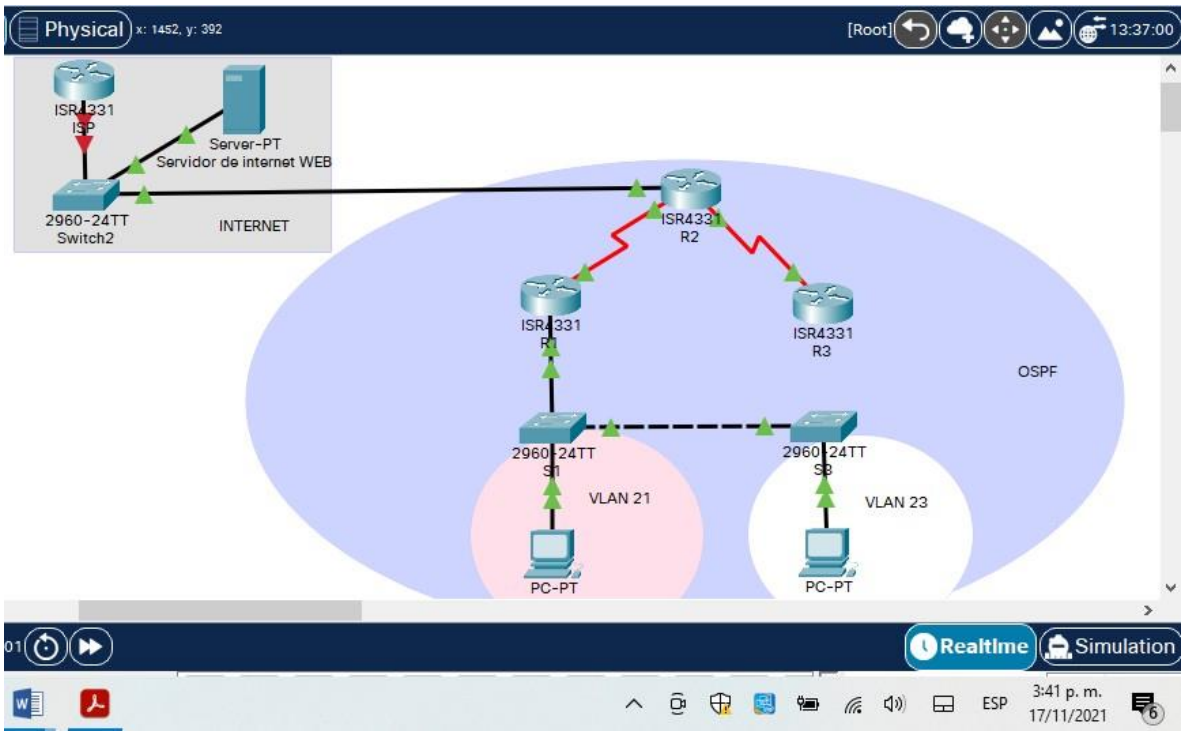


Fuente propia.

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. Durante la evaluación,probará y registrará la red mediante los comandos comunes de CLI.

Figura 8. Topología de red escenario 2.



Fuente propia.

Parte 1. Inicializar dispositivos

Paso 1. Inicializar y volver a cargar los routers y los switchs.

Tabla 4. Comandos de inicialización y recarga de routers y switches.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers y switches	erase startup-config
Volver a cargar todos los routers y switches	reload
Verificar que la base de datos de VLAN noesté en la memoria flash en ambos switches	show flash

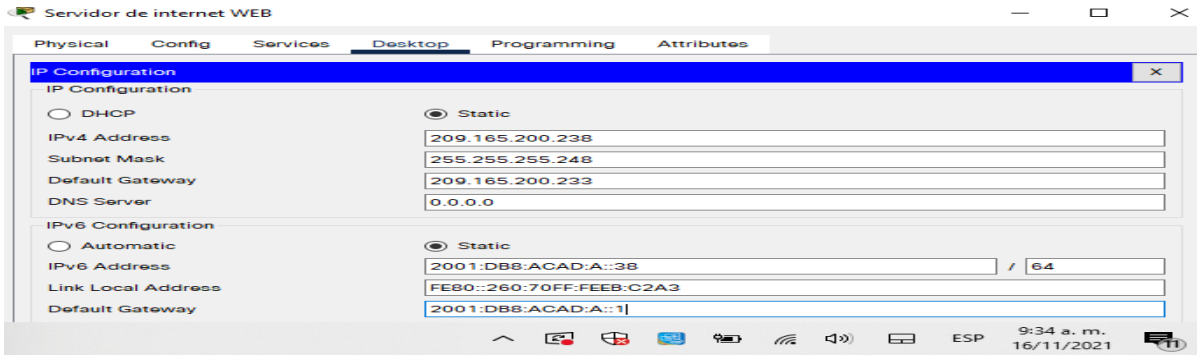
Parte 2. Configurar los parámetros básicos de los dispositivos.

Paso 1. Configurar la computadora de Internet.

Tabla 5. Configuración del 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

Figura 9. Configuración del servidor de internet.



Fuente propia.

Paso 2. Configuración básica R1

Comando	Descripción del comando
Router(config)#No ip domain-lookup	Desactiva la búsqueda DNS
Router(config)# Hostname R1	Se asigna nombre del router
R1(config)# Enable secret class	Se asigna Contraseña de exec privilegiado cifrada
R1(config)#Line console 0	Se accede a la linea de consola
R1(config-line)#Password cisco	Se asigna contraseña **cisco**
R1(config-line)#login	Se solicita autenticación
R1(config-line)# Line vty 0 4	Se accede a la linea acceso telnet
R1(config-line)# Password cisco	Se asigna contraseña **cisco**
R1(config-line)#login	Se solicita autenticación
R1(config)# service password-encryption	Se cifran las contraseñas de texto no cifrado
R1(config)#banner motd #se prohíbe el acceso no autorizado#	Se configura un mensaje motd de inicio
R1(config)#ipv6 unicast-routing	Se habilita router para ipv6
R1(config)# Interface s0/2/0	Se ingresar a la s0/2/0
R1(config-if)#description Interfaz serial 0/2/0	Se le asigna una descripción a la s0/2/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Se asigna dirección ipv4 y mascara a la s0/2/0
R1(config-if)#ipv6 address 2001:db8:acad:1::/64	Se asigna dirección ipv6 y mascara a la s0/2/0
R1(config-if)# clock rate 128000	Se establece la frecuencia de reloj en 128000
R1(config-if)#no shutdown	Se activa la interfaz s0/2/0

Paso 3. Configuración básica R2

Comando	Descripción del comando
Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Router(config)#hostname R2	Se asigna nombre del router
R2(config)#enable secret class	Se asigna Contraseña de exec privilegiado cifrada
R2(config)#line console 0	Se accede a la linea de consola
R2(config-line)#password cisco	Se asigna contraseña **cisco**
R2(config-line)#login	Se solicita autenticación
R2(config-line)#line vty 0 4	Se accede a la linea acceso telnet
R2(config-line)#password cisco	Se asigna contraseña **cisco**
R2(config-line)#login	Se solicita autenticación
R2(config)# service password-encryption	Se cifran las contraseñas de texto no cifrado
R2(config)# ip http server	Habilitar el servidor HTTP - Comando no admitido en el simulador.
R2(config)#banner motd #se prohíbe el acceso no autorizado.#	Se configura un mensaje motd de inicio
R2(config)#ipv6 unicast-routing	Se habilita router para ipv6
R2(config)#int s0/2/0	Se ingresa a la s0/2/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252	Se asigna dirección ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64	Se asigna dirección ipv6
R2(config-if)#no shutdown	Se activa la interfaz s0/2/0
R2(config)#interface s0/2/1	Se ingresa a la s0/2/1
R2(config-if)#ip address 172.16.2.1 255.255.255.252	Se asigna dirección ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64	Se asigna dirección ipv6
R2(config-if)#clock rate 128000	Se establece la frecuencia de reloj en 128000
R2(config-if)#no shutdown	Se activa la interfaz s0/2/1
R2(config)#interface g0/0/0	Se ingresa a la g0/0/0

R2(config-if)#description interface hacia internet	Se le asigna una descripción a g0/0/0
R2(config-if)#ip address 209.165.200.233 255.255.255.248	Se asigna dirección ipv4
R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/	Se asigna dirección ipv6
R2(config-if)#no shutdown	Se activa la interfaz g0/0/0
R2(config)#interface loopback 0	Se crea y activa la interfaz loopback 0
R2(config-if)#description servidor WEB	Se le asigna una descripción a lo 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255	Se asigna dirección ipv4
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0	Se le asigna ruta predeterminada ipv4 a g0/0/0
R2(config)#ipv6 route ::/0 G0/0/0	Se le asigna ruta predeterminada ipv6 a g0/0/0

Paso 4. Configuración básica R3

Comando	Descripción del comando
Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Router(config)#hostname R3	Se asigna nombre del router
R3(config)#enable secret class	Se asigna Contraseña de exec privilegiado cifrada
R3(config)#line console 0	Se accede a la linea de consola
R3(config-line)#password cisco	Se asigna contraseña **cisco**
R3(config-line)#login	Se solicita autenticación
R3(config-line)#line vty 0 4	Se accede a la linea acceso telnet
R3(config-line)#password cisco	Se asigna contraseña **cisco**
R3(config-line)#login	Se solicita autenticación
R3(config)# service password-encryption	Se cifran las contraseñas de texto no cifrado
R2(config)#banner motd #se prohíbe el acceso no autorizado.#	Se configura un mensaje motd de inicio
R3(config)#ipv6 unicast-routing	Se habilita router para ipv6
R3(config)#interface s0/2/1	Se activa la interfaz s0/2/1

R3(config-if)#ip address 172.16.2.2 255.255.255.252	Se asigna dirección ipv4
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64	Se asigna dirección ipv6
R3(config-if)#no shutdown	Se activa la interfaz s0/2/1
R3(config)#interface loopback 4	Se crea y activa la interfaz loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0	Se le asigna dirección ipv4
R3(config)#interface loopback 5	Se crea y activa la interfaz loopback 5
R3(config-if)#ip add 192.168.5.1 255.255.255.	Se le asigna dirección ipv4
R3(config)#interface loopback 6	Se crea y activa la interfaz loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0	Se le asigna dirección ipv4
R3(config)#interface loopback 7	Se crea y activa la interfaz loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64	Se le asigna dirección ipv6
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1	Se le asigna ruta predeterminada ipv4 a s0/2/1
R3(config)#ipv6 route ::/0 S0/2/1	Se le asigna ruta predeterminada ipv6 a s0/2/1

Paso 5. Configuración básica S1

Comando	Descripción del comando
Switch(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Switch (config)#hostname S1	Se asigna nombre del switch
S1(config)#enable secret class	Se asigna Contraseña de exec privilegiado cifrada
S1(config)#line console 0	Se accede a la linea de consola
S1(config-line)#password cisco	Se asigna contraseña **cisco**
S1(config-line)#login	Se solicita autenticación
S1(config-line)#line vty 0 4	Se accede a la linea acceso telnet
S1(config-line)#password cisco	Se asigna contraseña **cisco**
S1(config-line)#login	Se solicita autenticación

S1(config)# service password-encryption	Se cifran las contraseñas de texto no cifrado
S1(config)#banner motd #se prohíbe el acceso no autorizado.#	Se configura un mensaje motd de inicio

Paso 6. Configuración básica S3

Comando	Descripción del comando
Switch(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Switch (config)#hostname S3	Se asigna nombre del switch
S3(config)#enable secret class	Se asigna Contraseña de exec privilegiado cifrada
S3(config)#line console 0	Se accede a la linea de consola
S3(config-line)#password cisco	Se asigna contraseña **cisco**
S3(config-line)#login	Se solicita autenticación
S3(config-line)#line vty 0 4	Se accede a la linea acceso telnet
S3(config-line)#password cisco	Se asigna contraseña **cisco**
S3(config-line)#login	Se solicita autenticación
S3(config)# service password-encryption	Se cifran las contraseñas de texto no cifrado
S3(config)#banner motd #se prohíbe el acceso no autorizado.#	Se configura un mensaje motd de inicio

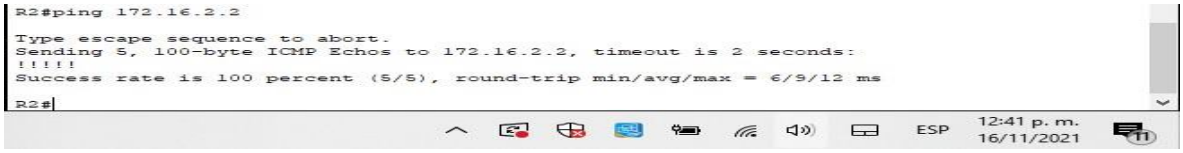
Paso 7 verificar la conectividad de la red

Desde	A	Dirección IP	Resultados del Ping
R1	R2, S0/2/0	172.16.1.2	100 % (5/5)
R2	R3, S0/0/1	172.16.2.2	100 % (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233	Send = 4 Received = 4

Figura 10. Ping desde R1 a R2.

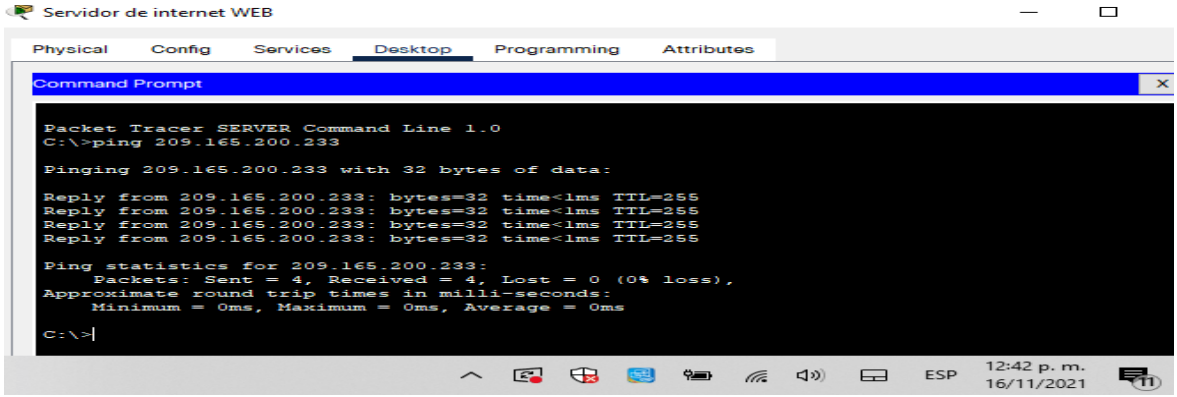
Fuente propia.

Figura 11. Ping desde R2 a R3.



Fuente propia.

Figura 12. Ping desde 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 la seguridad del switch, las VLAN y el routing entre VLAN de S1

Comando	Descripción del comando
S1(config)#vlan 21	Se crea vlan 21
S1(config-vlan)#name contabilidad	Se asigna nombre contabilidad a vlan 21
S1(config-vlan)#vlan 23	Se crea vlan 23
S1(config-vlan)#name ingenieria	Se asigna nombre ingenieria a vlan 23
S1(config-vlan)#vlan 99	Se crea vlan 99
S1(config-vlan)#name administración	Se asigna nombre administracion a vlan 99
S1(config)#interface vlan 99	Se ingresa a vlan 99 para configurar
S1(config-if)#ip address 192.168.99.2 255.255.255.0	Se asigna dirección ipv4 a vlan 99
S1(config-if)#no shutdown	Se activa la interfaz
S1(config)#ip default-gateway 192.168.99.1	Se asigna la gateway al dispositivo
S1(config)#interface f0/3	Se ingresa a la interfaz f0/3
S1(config-if)#switchport mode trunk	Se crea enlace troncal en f0/3
S1(config-if)#switchport trunk native vlan 1	Se asigna vlan 1 como vlan nativa en f0/3
S1(config)#interface f0/5	Se ingresa a la interfaz f0/5
S1(config-if)#switchport mode trunk	Se crea enlace troncal en f0/5
S1(config-if)#switchport trunk native vlan 1	Se asigna vlan 1 como vlan nativa en f0/5
S1(config)#interface range f0/1- f0/2	Se ingresa al rango de interfaces f0/1 a f0/2
S1(config-if-range)#switchport mode access	Se configuran f0/1 a f0/2 como puertos de acceso
S1(config)#interface range f0/7- f0/24	Se ingresa al rango de interfaces f0/7 a f0/24
S1(config-if-range)#switchport mode access	Se configuran f0/7 a f0/24 como puertos de acceso
S1(config)#interface f0/6	Se ingresa a la interfaz f0/6
S1(config-if)#switchport mode access vlan 21	Se asigna f0/6 a vlan 21
S1(config)#interface range f0/7 - f0/24	Se ingresa al rango de interfaces f0/7 a f0/24
S1(config-if-range)#shutdown	Se apaga el rango de interfaces f0/7 a f0/24

Paso 2. Configurar la seguridad del switch, las VLAN y el routing entre VLAN de S3

Comando	Descripción del comando
S3(config)#vlan 21	Se crea vlan 21
S3(config-vlan)#name contabilidad	Se asigna nombre contabilidad a vlan 21
S3(config-vlan)#vlan 23	Se crea vlan 23
S3(config-vlan)#name ingenieria	Se asigna nombre ingenieria a vlan 23
S3(config-vlan)#vlan 99	Se crea vlan 99
S3(config-vlan)#name administración	Se asigna nombre administracion a vlan 99
S3(config)#interface vlan 99	Se ingresa a vlan 99 para configurar
S3(config-if)#ip address 192.168.99.3 255.255.255.0	Se asigna dirección ipv4 a vlan 99
S3(config-if)#no shutdown	Se activa la interfaz
S3(config)#ip default-gateway 192.168.99.1	Se asigna la gateway al dispositivo
S3(config)#interface f0/3	Se ingresa a la interfaz f0/3
S3(config-if)#switchport mode trunk	Se crea enlace troncal en f0/3
S3(config-if)#switchport trunk native vlan 1	Se asigna vlan 1 como vlan nativa en f0/3
S3(config)#interface range f0/1- f0/2	Se ingresa al rango de interfaces f0/1 a f0/2
S3(config-if-range)#switchport mode access	Se configuran f0/1 a f0/2 como puertos de acceso
S3(config)#interface range f0/7- f0/24	Se ingresa al rango de interfaces f0/7 a f0/24
S3(config-if-range)#switchport mode access	Se configuran f0/7 a f0/24 como puertos de acceso
S3(config)#interface f0/18	Se ingresa a la interfaz f0/18
S3(config-if)#switchport mode access vlan 21	Se asigna f0/18 a vlan 21
S3(config)#interface range f0/7 - f0/17	Se ingresa al rango de interfaces f0/7 a f0/17
S3(config-if-range)#shutdown	Se apaga el rango de interfaces f0/7 a f0/17
S3(config)#interface range f0/19 - f0/24	Se ingresa al rango de interfaces f0/19 a f0/24
S3(config-if-range)#shutdown	Se apaga el rango de interfaces f0/19 a f0/24

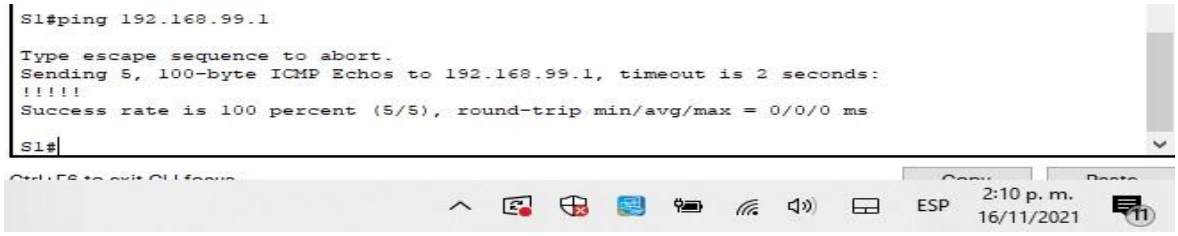
Paso 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN de R1

Comando	Descripción del comando
R1(config)#interface g0/0/1	Se ingresa a la interface g0/0/1
R1(config)#no shutdown	Se activa la interface g0/0/1
R1(config)#interface g0/0/1.21	Se crea la subinterfaz g0/0/1.21
R1(config-subif)#description Lan contabilidad	Se le asigna una descripción a la subinterfaz g0/0/1.21
R1(config-subif)#encapsulation dot1q 21	Se le aplica encapsulación a la subinterfaz g0/0/1.21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0	Se le asigna dirección ipv4 a la subinterfaz g0/0/1.21
R1(config)#interface g0/0/1.23	Se crea la subinterfaz g0/0/1.23
R1(config-subif)#description Lan ingenieria	Se le asigna una descripción a la subinterfaz g0/0/1.23
R1(config-subif)#encapsulation dot1q 23	Se le aplica encapsulación a la subinterfaz g0/0/1.23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0	Se le asigna dirección ipv4 a la subinterfaz g0/0/1.23
R1(config)#interface g0/0/1.99	Se crea la subinterfaz g0/0/1.99
R1(config-subif)#description Lan administracion	Se le asigna una descripción a la subinterfaz g0/0/1.99
R1(config-subif)#encapsulation dot1q 99	Se le aplica encapsulación a la subinterfaz g0/0/1.99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0	Se le asigna dirección ipv4 a la subinterfaz g0/0/1.99

Paso 4 verificar la conectividad de la red.

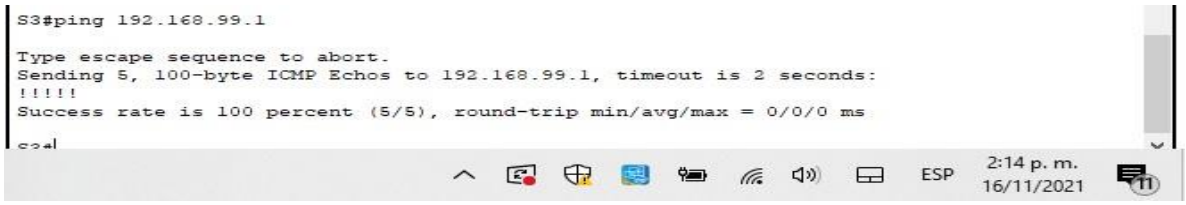
Desde	A	Dirección IP	Resultado del ping
S1	R1, dirección VLAN 99	192.168.99.1	100 porcent (5/5)
S3	R1, dirección VLAN 99	192.168.99.1	100 porcent (5/5)
S1	R1, dirección VLAN 21	192.168.21.1	100 porcent (5/5)
S3	R1, dirección VLAN 23	192.168.23.1	100 porcent (5/5)

Figura 13. Ping de S1 a R1 vlan 99



Fuente propia.

Figura 14. Ping de S3 a R1 vlan 99

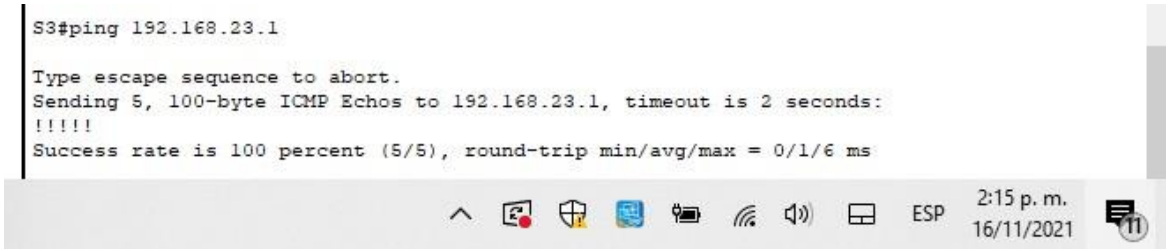


Fuente propia.

Figura 15. Ping de S1 a R1 vlan 21

Fuente propia.

Figura 16. Ping de S3 a R1 vlan 23



Fuente propia

Parte 4. Configurar el protocolo de routing dinámico OSPF

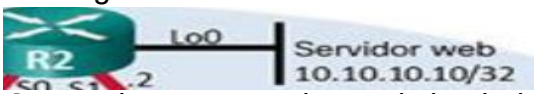
Paso 1. Configurar OSPF en el R1

Comando	Descripción del comando
R1(config)#router ospf 73	Se activa protocolo ospf en R1
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0	Se asigna red 192.168.21.0 conectada directamente
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0	Se asigna red 192.168.23.0 conectada directamente
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0	Se asigna red 192.168.99.0 conectada directamente
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0	Se asigna red 172.16.1.0 0.0.0.3 conectada directamente
R1(config-router)#passive-interface g0/0/1	Se establece interfaz Lan g0/0/1 como pasiva
R1(config-router)#passive-interface g0/0/1.21	Se establece interfaz Lan g0/0/1.21 como pasiva
R1(config-router)#passive-interface g0/0/1.23	Se establece interfaz Lan g0/0/1.23 como pasiva
R1(config-router)#passive-interface g0/0/1.99	Se establece interfaz Lan g0/0/1.99 como pasiva
Desactivar la sumarización	Comando no aceptado en el simulador.

Paso 2. Configurar OSPF en el R2

Comando	Descripción del comando
R2(config)#router ospf 73	Se activa protocolo ospf en R2
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0	Se asigna red 10.10.10.10 conectada directamente
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0	Se asigna red 172.16.1.0 conectada directamente
R2(config-router)#net 172.16.2.0 0.0.0.3 area 0	Se asigna red 172.16.2.0 conectada directamente
R2(config-router)#passive-interface loopback 0	Se establece interfaz lo 0 como pasiva
Desactivar la sumarización	Comando no aceptado en el simulador.

Paso 3. Configurar OSPFv3 en el R2

Comando	Descripción del comando
R2(config)#ipv6 router ospf 74	Se activa protocolo ospfv3 en R2
R2(config-rtr)#router-id 1.1.1.1	Se asigna id 1.1.1.1 a router
R2(config)#interface s0/2/0	Se ingresa a s0/2/0
R2(config-if)#ipv6 ospf 74 area 0	Se asigna red conectada directamente
R2(config)#interface s0/2/01	Se ingresa a s0/2/1
R2(config-if)#ipv6 ospf 74 area 0	Se asigna red conectada directamente
R2(config)#interface g0/0/0	Se ingresa a g0/0/0
R2(config-if)#ipv6 ospf 74 area 0	Se asigna red conectada directamente
Establecer todas las interfaces de LAN IPv4 (Loopback)como pasivas	
Desactivar la sumarización	Comando no aceptado en el simulador.

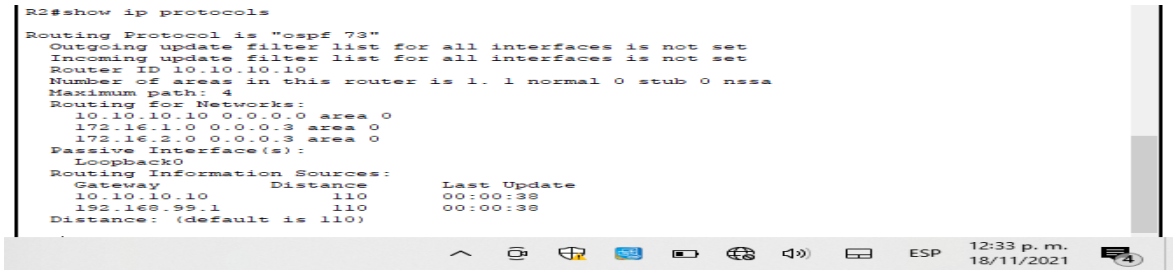
Paso 4. Configurar OSPFv3 en el R3

Comando	Descripción del comando
R3(config)#ipv6 router ospf 74	Se activa protocolo ospfv3 en R3
R3(config-rtr)#router-id 2.2.2.2	Se asigna id 2.2.2.2 a router
R3(config)#interface s0/2/1	Se ingresa a s0/2/1
R3(config-if)#ipv6 ospf 74 area 0	Se asigna red conectada directamente
R3(config)#ipv6 router ospf 74	Se ingresa al router para configurar inrerfaces
R3(config-rtr)#passive-interface lo 4	Se establece interfaz lo 4 como pasiva
R3(config-rtr)#passive-interface lo 5	Se establece interfaz lo 5 como pasiva
R3(config-rtr)#passive-interface lo 6	Se establece interfaz lo 6 como pasiva
Desactive la sumarización automática.	En este protocolo eso no se hace para eso se coloca la wildcard y en IPV6 no se hace.

Paso 4. Verificar la información de OSPF

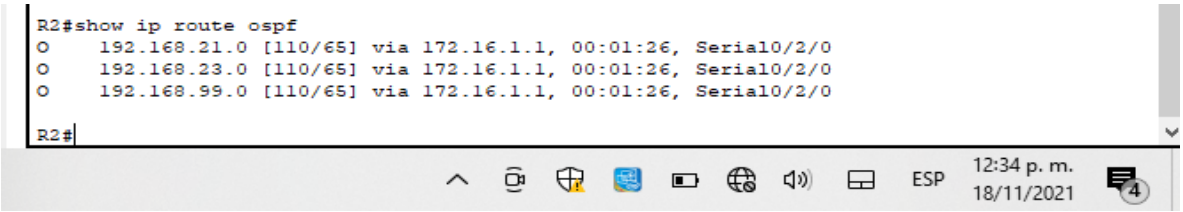
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradasen un router?	show ip protocols show run
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuraciónen ejecución?	Show run show running-config

Figura 17. Comando show ip protocols



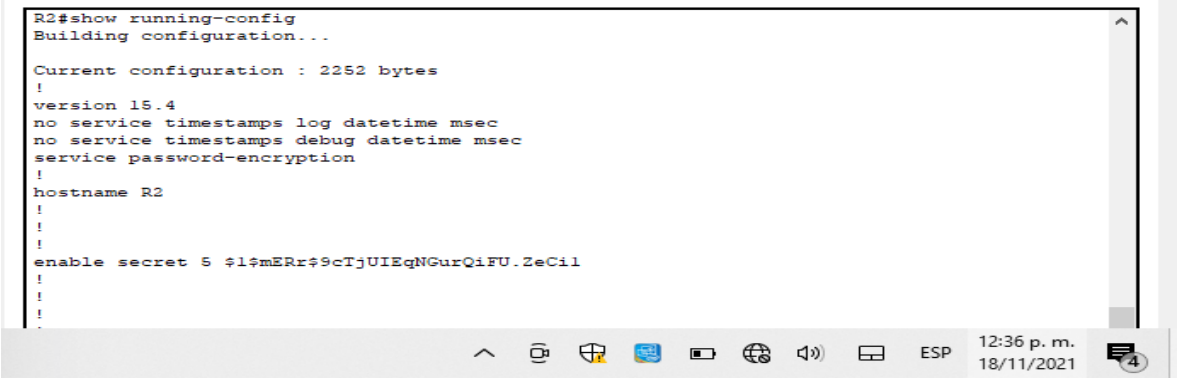
Fuente propia.

Figura 18. Comando show ip route ospf



Fuente propia.

Figura 19. Comando show running-config (show run)



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

Comando	Descripción del comando
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20	Se reservan las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20	Se reservan las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas
R1(config)#ip dhcp pool ACCT	Se crea el pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0	Se asigna la red 192.168.21.0/24

R1(dhcp-config)#domain-name ccna-sa.com	Se crea el dominio con nombre ccna-sa.com
R1(dhcp-config)#dns-server 10.10.10.10	Se asigna servidor dns 10.10.10.10
R1(dhcp-config)#default-router 192.168.21.1	Se asigna router por defecto 192.168.21.1
R1(config)#ip dhcp pool ENGNR	Se crea el pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0	Se asigna la red 192.168.23.0 /24
R1(dhcp-config)#dns-server 10.10.10.10	Se asigna servidor dns 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com	Se crea el dominio con nombre ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1	Se asigna router por defecto 192.168.23.1

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

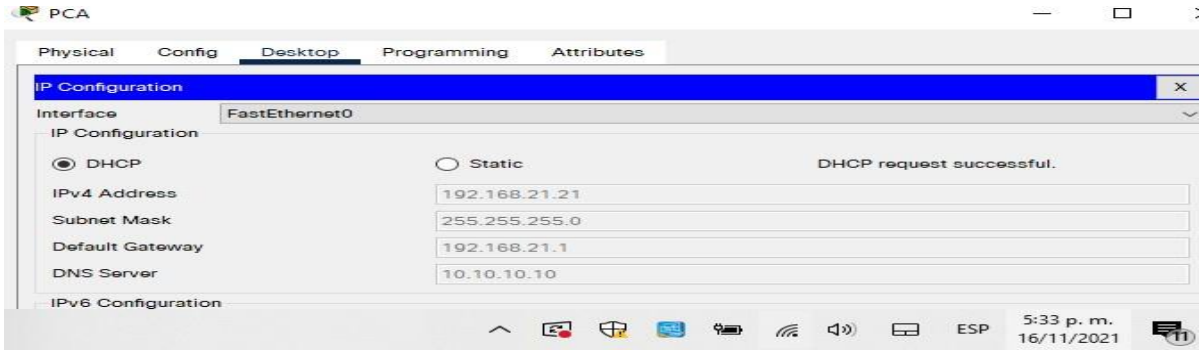
Comando	Descripción del comando
R2(config)#username webuser privilege 15 password cisco12345	Se crea una base de datos local con una cuenta de usuario
R2(config)#ip http server	Habilitar el servicio del servidor HTTP (Comando inhabilitado en el simulador)
R2(config)#ip http authentication local	Configurar el servidor HTTP para utilizar la base de datos local para la autenticación (Comando inhabilitado en el simulador)
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233	Se crea una NAT estática al servidor web.
R2(config)#interface g0/0/0	Se ingresa a la interfaz g0/0/0
R2(config-if)#ip nat outside	Se asigna como interfaz externa
R2(config-if)#interface s0/2/0	Se ingresa a la interfaz s0/2/0
R2(config-if)#ip nat inside	Se asigna como interfaz interna
R2(config-if)#interface s0/2/1	Se ingresa a la interfaz s0/2/1
R2(config-if)#ip nat inside	Se asigna como interfaz interna
R2(config-if)#interface lo 0	Se ingresa a la interfaz lo 0

R2(config-if)#ip nat inside	Se asigna como interfaz interna
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Se crea primera lista de acceso
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	Se crea segunda lista de acceso
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255	Se crea tercera lista de acceso
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248	Se define el pool de direccione publicas INTERNET
R2(config)#ip nat inside source list 1 pool INTERNET	Se define la traducción nat dinámica para el pool INTERNET

Paso 3. Verificar el protocolo DHCP y la NAT estática

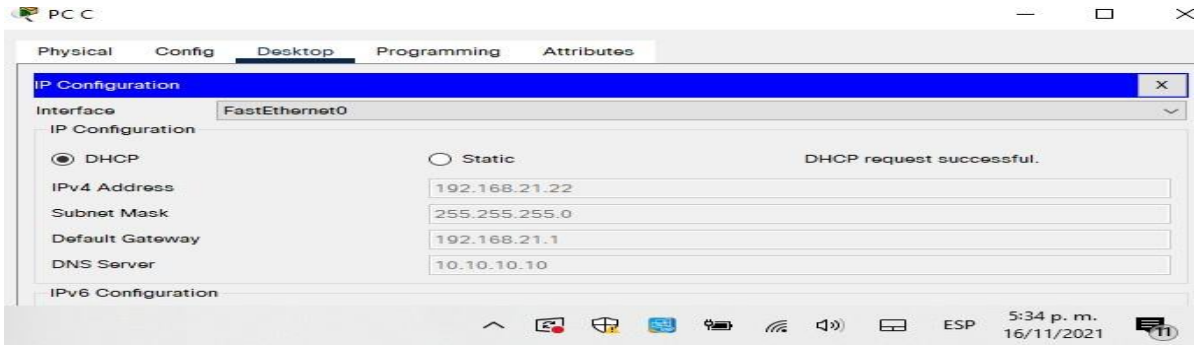
Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Asigna dirección dhcp 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Asigna dirección dhcp 192.168.21.22
Verificar que la PC-A pueda hacer ping ala PC-C **Nota:** Quizá sea necesario deshabilitar elfirewall de la PC.	Send = 4, Received = 4
Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.238) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Acceso exitoso a http://209.165.200.238

Figura 20. DHCP PC-A



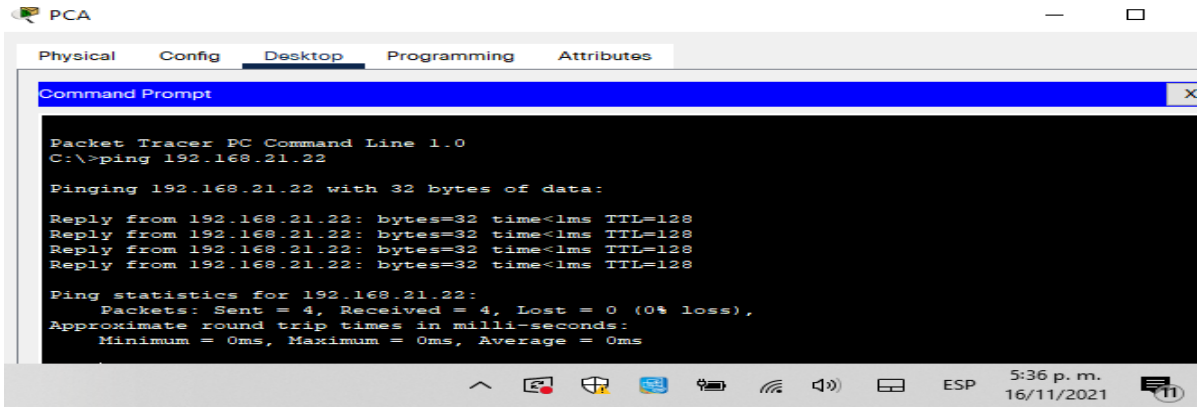
Fuente propia.

Figura 21. DHCP PC-C



Fuente propia.

Figura 22. Ping de PC-A a PC-C



Fuente propia.

Figura 23. Acceso a http://209.165.200.238

Fuente propia.

Parte 6. Configurar NTP

Comando	Descripción del comando
R2#clock set 09:00:00 05 march 2016	Se ajusta la fecha de R2
R2(config)#ntp master 5	Se configura R2 como maestro NTP
R1(config)#ntp server 172.16.1.2	Se configura R1 como cliente NTP
R1(config)#ntp update-calendar	Se solicitan actualizaciones de calendario NTP en R1
R1#show clock	Se muestra hora en R1 9:4:47.679 UTC Sat Mar 5 2016

Figura 24. Show clock

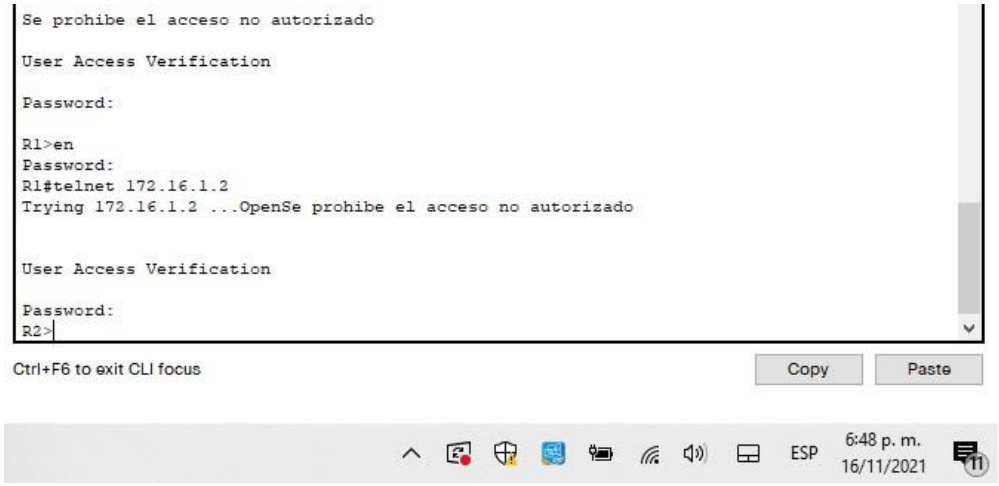
Fuente propia.

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

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

Comando	Descripción del comando
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Se crea lista de acceso 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	Se crea lista de acceso 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255	Se crea lista de acceso 192.168.0.0 0.0.3.255
R2(config)#ip access-list standard ADMIN-MGT	Se configura la lista estándar ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1	Se permite el host 172.16.1.1
R2(config-std-nacl)#deny any	Se deniega el acceso a lo demás
R2(config)#line vty 0 4	Se ingresa a la línea de telnet
R2(config-line)#ip access-class ADMIN-MGT in	Se aplica la ACL con nombre a las líneas VTY
R2(config-line)#transport input telnet	Se permite el acceso por telnet
R1#telnet 172.16.1.2	Se verifica que la acl funcione como se espera: Trying 172.16.1.2 ...Open User Access Verification Password:

Figura 25. Telnet 172.16.1.2



Fuente propia.

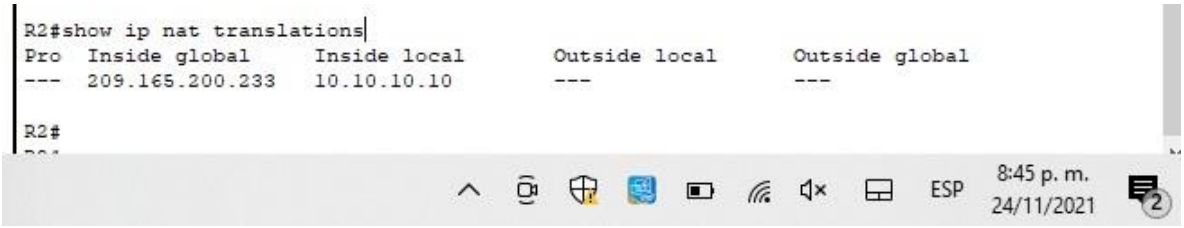
Paso 2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas poruna lista de acceso desde la última vez que se restableció	R2#show Access-list
Restablecer los contadores de una listade acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la direcciónen que se aplica?	R2#show run
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?	R2#clear ip nat translation

Figura 26. Comando show access-list

Fuente propia.

Figura 27. Show ip nat translations



Fuente propia.

CONCLUSIONES

Dentro del desarrollo de los dos escenarios desmenuzamos varios temas claves, no solo con el conocimiento básico de infraestructura, también protocolos de comunicación, seguridad, enrutamiento y controles de acceso. Todos estos temas de vital importancia para la optimización de recursos, disminución de costos y seguridad de la información.

Pudimos diferenciar y aplicar los protocolos ipv4 e ipv6, aplicando los dos tipos de direcciones, conociendo así el crecimiento exponencial en las redes, asimilando también las nomenclaturas de cada una y de las máscaras de red. Se configuraron aspectos básicos, de seguridad, de enrutamiento y comunicación cliente/servidor de los dispositivos involucrados en la red como lo fueron computadores, servidores, routers y switches. Basados en protocolos como el OSPF vital para la comunicación en la red y la asignación dinámica de direcciones, basados en el uso de routers como servidores de servicios DHCP, lo cual logro optimizar un dispositivo de enrutamiento para que brindara un servicio adicional.

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] Comandos básicos para trabajar con Packet Tracer « EL portafolio de las redes. (wordpress.com)

[9] CIPA desarrollo actividad intermedia personalizada (2021-10-16 at 13:04 GMT-7) Google Drive

[10] https://ejemplos.net/ejemplo-de-abstrac/#:~:text=Abstract.%20Es%20la%20expresi%C3%B3n%20que%20hace%20referencia%20a,un%20trabajo%20de%20mayor%20alcance%20o%20m%C3%A1s%20grande.

[11] http://normas-apa.com/resumen-trabajo-escrito/#:~:text=El%20resumen%20de%20un%20trabajo%20escrito%20es%20un,en%20el%20que%20se%20explican%20sus%20ideas%20principales.

[12] Sustentación Jair Hernández escenarios 1 y 2 Diplomado CCNA CISCO - UNAD – YouTube

[13] Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

[14] Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx