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

JHEYSON SANCHEZ DIAZ

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

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

JHEYSON SANCHEZ DIAZ

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

DIRECTORA:
Ing. NANCY AMPARO GUACA G

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

VALLEDUPAR, 01 de diciembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BIT: En informática y otras disciplinas, unidad mínima de información, que puede tener solo dos valores (cero o uno).

CISCO: Es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red. La palabra Cisco proviene del nombre de la ciudad de San Francisco, lugar donde se fundó la empresa.

DOMINIO: En informática, parte de una dirección de Internet que identifica un sitio web y que describe el tipo de empresa u organización a la que pertenece o bien el país donde está registrado.

DNS: Corresponde a las siglas en inglés de "Domain Name System", es decir, "Sistema de nombres de dominio". Este sistema es básicamente la agenda telefónica de la Web que organiza e identifica dominios.

ROUTER: Es un dispositivo que administra el tráfico de datos que circula en una red de computadoras. Router es un anglicismo que significa enrutador o direccionador.

SSH: Es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

SWITCH: Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet

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

VTY: Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15.

RESUMEN

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

En el segundo escenario se configurará 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.

En este trabajo se presenta un avance correspondiente al desarrollo de la temática establecida como alternativa de grado, con la modalidad adoptada por el diplomado de profundización llamada “Proyecto Aplicado”, en donde el director del curso propone dos escenarios con características y requerimientos específicos, en donde el primer escenario será desarrollado acorde con las temáticas del módulo 1. Aplicando los conocimientos adquiridos en las Unidades 1, 2, 3, 4, 5. El segundo escenario será desarrollado acorde con las temáticas del módulo 2. Aplicando los conocimientos adquiridos en las Unidades 6, 7, 8, 9, 10.

Palabras Clave: CISCO, CCNA, Enrutamiento, Redes, Sistemas.

SUMMARY

In the first scenario, the devices on a small network will be configured. A router, switch and equipment must be configured, and the IPv4 addressing scheme for the proposed LANs must be designed. The router and switch must also be managed securely.

The second scenario will configure a small network to support IPv4 and IPv6 connectivity, switch security, routing between VLANs, OSPF dynamic routing protocol, dynamic host configuration protocol (DHCP), dynamic and static network address (NAT) translation, access control (ACL) and server/client network time protocol (NTP). During the evaluation, you will test and register the network using the common CLI commands.

This paper presents an advance corresponding to the development of the theme established as a grade alternative, the modality adopted by the deepening diploma called "Applied Project", where the course director proposes two scenarios with specific characteristics and requirements, where the first scenario will be developed according to the themes of module 1. Applying the knowledge acquired in Units 1, 2, 3, 4, 5. The second scenario will be developed according to the themes of module 2. Applying the knowledge acquired in Units 6, 7, 8, 9, 10.

Keywords: CISCO, CCNA, Routing, Networks, Systems.

INTRODUCCIÓN

En este trabajo se utilizará la modalidad “Proyecto Aplicado”, en donde la directora del curso propone dos escenarios con características y requerimientos específicos con el fin de utilizar herramientas de simulación y laboratorios de acceso remoto para establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

Los objetivos específicos que se pretenden alcanzar con el desarrollo del escenario 1 en este trabajo son: Construir en el simulador la Red, desarrollar el esquema de direccionamiento IP para las redes LAN, configurar los aspectos básicos de los dispositivos de Red, configurar los ajustes básicos de seguridad en un router y un switch, configurar los hosts y verificar la conectividad entre los equipos.

Los objetivos a enfatizar en el desarrollo del escenario 2, son los siguientes: diseñar políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.
Asimismo, se busca configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.
También, se pretende diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.

DESARROLLO

Escenario 1

Topología

Figura 1. Topología escenario 1

Fuente. propia

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.
Aspectos básicos/situación
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

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.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.
Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Tabla de direccionamiento

Item	Requerimiento	Respuesta
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.53.0
Requerimiento de host Subred LAN1	100	

Requerimiento de host Subred LAN2	50	
R1 G0/0/1	Primera dirección de host de la subred LAN1	192.168.53.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2	192.168.53.129/26
S1 SVI	Segunda dirección de host de la subred LAN1	192.168.53.2/25
PC-A	Última dirección de host de la subred LAN1	192.168.53.126/25
PC-B	Última dirección de host de la subred LAN2	192.168.53.190/26

Fuente. propia

Parte 3: Configure aspectos básicos
Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.
Configuración del Router R1:

Tabla 2. Comandos para configuración del Router R1 por consola desde el PC-B:

COMANDO	DESCRIPCIÓN DEL COMANDO
Router>enable	Ingresa a modo privilegiado
Router#configure terminal	Ingresa a modo de configuración
Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Router(config)#hostname R1	Asigna Nombre del router: R1
R1(config)#ip domain-name ccna-lab.com	Nombra el dominio del router R1: ccna-lab.com
R1(config)#enable secret ciscoenpass	Activa contraseña cifrada para el modo EXEC privilegiado - Password: ciscoenpass
R1(config)#line console 0	Ingresa a configuración de consola
R1(config-line)#password ciscoconpass	Contraseña de acceso a la consola - Password: ciscoconpass
R1(config-line)#login	Habilita contraseña
R1(config-line)#exit	Sale de consola para volver a modo de configuración
R1(config)#security passwords min-length 10	Establece la longitud mínima para las contraseñas 10 caracteres
R1(config)#username admin password admin1pass	Crea un usuario administrativo en la base de datos local - Nombre de usuario: admin - Password: admin1pass
R1(config)#line vty 0 4	Sube líneas del router desde 0 hasta 4

R1(config-line)#password ciscocisco	Asigna contraseña: ciscocisco
R1(config-line)#login local	Configura el inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#transport input SSH	Configura VTY solo aceptando SSH
R1(config-line)#exit	Sale de líneas VTY para volver a modo de configuración
R1(config)#service password-encryption	Cifra las contraseñas de texto no cifrado
R1(config)#banner motd #Este es un Router privado, acceso denegado#	Configura un MOTD Banner con el texto: Este es un Router privado, acceso denegado
R1(config)#interface gigabitEthernet 0/0/0	Ingresa a configuración de la interfaz Gig 0/0/0
R1(config-if)#ip address 192.168.53.129 255.255.255.192	Configura interfaz G0/0/0 - Establece la dirección IPv4
R1(config-if)#description esta es la interfaz de la LAN 2	Configura interfaz G0/0/0 - Establece la descripción
R1(config-if)#no shutdown	Configura interfaz G0/0/0 - Activa la interfaz
R1(config)#interface gigabitEthernet 0/0/1	Ingreso a configuracion de la interfaz Gig 0/0/1
R1(config-if)#description esta es la interfaz de la LAN 1	Configura interfaz G0/0/1 - Establece la descripción
R1(config-if)#ip address 192.168.53.129 255.255.255.192	Configura interfaz G0/0/1 - Establece la dirección IPv4
R1(config-if)#no shutdown	Configura interfaz G0/0/1 - Activa la interfaz.
R1(config)#ip domain name ccna-lab.com	Llama al dominio ccna-lab.com
R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024	Genera una clave de cifrado RSA - Módulo de 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	
R1#wr Building configuration... [OK]	Guarda la configuración en memoria

Fuente. propia

Configuración del Switch S1:

Tabla 3. Comandos para configuración de Switch S1 por consola desde el PC-A:

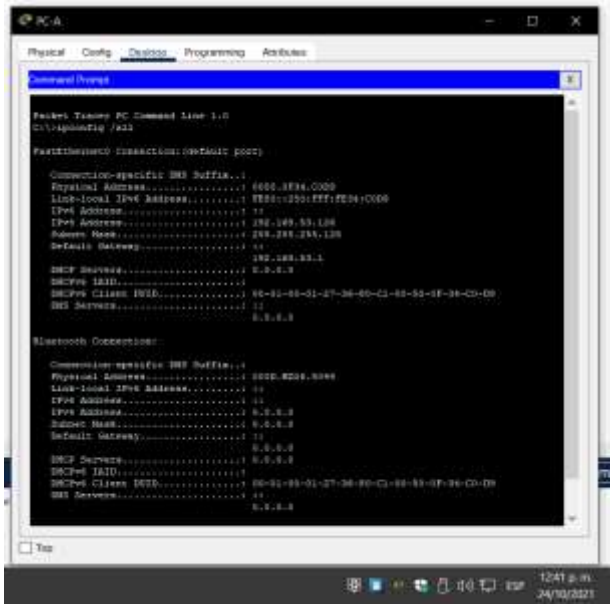
COMANDO	DESCRIPCIÓN DEL COMANDO
Switch>enable	Ingresa a modo privilegiado
Switch#configure terminal	Ingresa a modo de configuración
Switch(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Switch(config)#hostname S1	Asigna nombre al switch: S1
S1(config)#ip domain-name ccna-lab.com	Asigna nombre de dominio: ccna-lab.com
S1(config)#enable secret ciscoenpass	Activa contraseña cifrada para el modo EXEC privilegiado, Password: ciscoenpass
S1(config)#line console 0	Ingresa a la consola
S1(config-line)#password ciscoconpass	Asigna contraseña de acceso a la consola, Password: ciscoconpass
S1(config-line)#login	Habilita contraseña
S1(config-line)#exit	Sale de consola para volver a modo de configuración
S1(config)#username admin password admin1pass	Crea un usuario administrativo en la base de datos local, Nombre de usuario: admin Password: admin1pass
S1(config)#line vty 0 15	Sube líneas del switch desde 0 15
S1(config-line)#password ciscocisco	Asigna contraseña: ciscocisco
S1(config-line)#login local	Configura el inicio de sesión en las líneas VTY para que use la base de datos local
S1(config-line)#transport input ssh	Configura las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line)#exit	Sale de líneas vty para volver a modo de configuración
S1(config)#service password-encryption	Cifra las contraseñas de texto no cifrado
S1(config)#banner motd #Este es un Switch privado, acceso denegado#	Configura un MOTD Banner con el texto: Este es un Switch privado, acceso denegado
S1(config)#ip domain name ccna-lab.com	Llama al dominio ccna-lab.com
S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	Genera una clave de cifrado RSA - Módulo de 1024 bits
S1(config)#interface vlan 1	Ingresa a configuración de la vlan 1
S1(config-if)#ip address 192.168.53.2 255.255.255.128	Configura la interfaz de administración (SVI) Estableciendo la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
S1(config-if)#no sh	Activa la interfaz
S1(config-if)#exit	Sale de la interfaz vlan 1 para volver a modo de configuración
S1(config)#ip default-gateway 192.168.53.1	Configura la puerta de enlace predeterminada conforme a la tabla de direccionamiento
S1(config)#exit	Sale del modo de configuración
S1#wr Building configuration... [OK]	Guarda la configuración en memoria

Fuente. propia

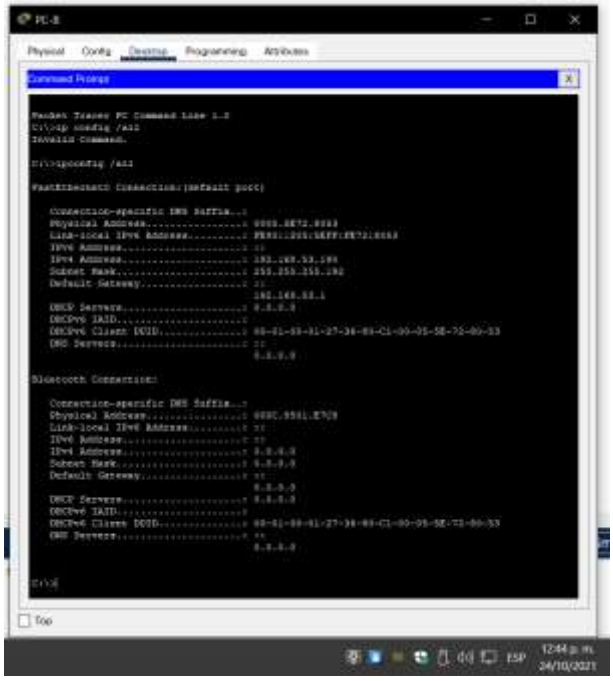
Paso 2. Configurar los equipos
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Figura 2. Evidencia de la configuración del PC - A



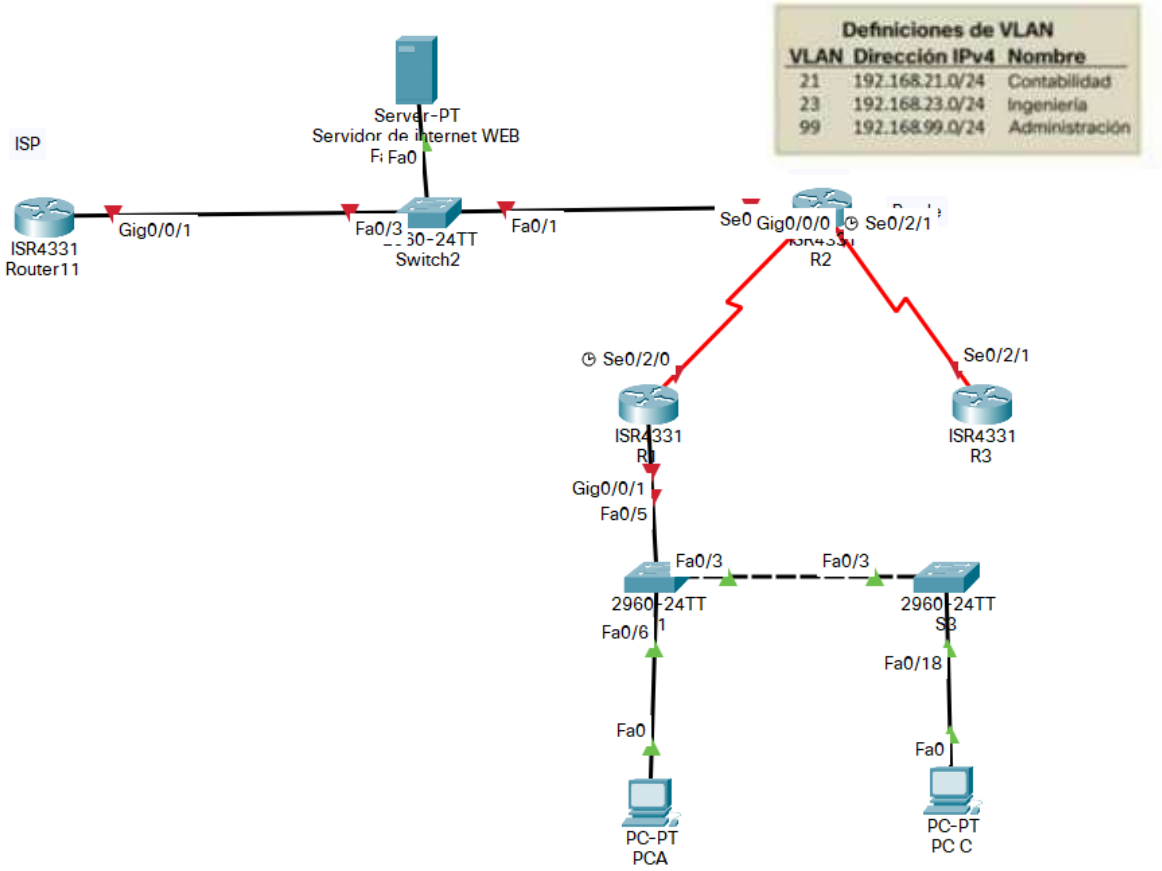
Fuente. Propia.

Figura 3. Evidencia de la configuración del PC – B



Fuente. Propia.

Escenario 2
Topología



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. Escenario 2, parte 1, tareas paso 1

Tarea	**Comando de IOS**
Elimina el archivo startup-config de todos los routers	Router>enable Router# erase startup-config
Volver a cargar todos los routers	Router#reload
Elimina el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch# erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload

Verifica que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash

Fuente. Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 5. Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

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

Fuente. Propia

Paso 2: Configurar R1

Tabla 6. Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactiva la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R1	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada: class	R1(config)#enable secret class
Contraseña de acceso a la consola cisco	R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)# login
Contraseña de acceso Telnet cisco	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifra las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado #
Interfaz S0/2/0	R1(config)# inter s0/2/0 R1(config-if)# description conección a R2 R1(config-if)#Ip address 172.16.1.1 255.255.255.252

	R1(config-if)#Ipv6 address 200:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut down Establece la descripción Establece la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establece la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establece la frecuencia de reloj en 128000 Activa la interfaz
Rutas predeterminadas	Configura una ruta IPv4 predeterminada de S0/2/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 Configura una ruta IPv6 predeterminada de S0/2/0 R1(config)#ipv6 route ::/0 s0/0/0

Fuente. Propia

Paso 3: Configurar R2

Tabla 7 La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactiva la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada : class	R2(config)#enable secret class
Contraseña de acceso a la consola : cisco	R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)# login
Contraseña de acceso Telnet : cisco	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifra las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilita el servidor HTTP	R2(config)#ip http server (este comando no lo permite el simulador)

Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado #
Interfaz S0/2/0	R2(config)#int s0/2/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown Establece la descripción Establece la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establece la dirección IPv6. Segun el diagrama de topología. Activa la interfaz
Interfaz S0/2/1	R2(config-if)#int s0/2/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown Establece la descripción Establece la dirección IPv4. Se uitiliza la primera dirección disponible en la subred. Establece la dirección IPv6. Usando el diagrama de topología para conocer la información de direcciones. Establece la frecuencia de reloj en 128000. Activa la interfaz
Interfaz G0/0/0 (simulación de Internet)	R2(config-if)# int g0/0/0 R2(config-if)# description Connection to Internet R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)# no shutdown Establece la descripción. Establece la dirección IPv4. Se utiliza la primera dirección disponible en la subred. Establece la dirección IPv6. Se utilizar la primera dirección disponible en la subred. Activa la interfaz

Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)#%LINK-5-CHANGED: Interface Loopback0, changed state to up%LINEPROTO-5-UPDOWN: Line Interface Loopback0, changed state to up R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit Establece la descripción. Establece la dirección IPv4. Exit para salir.
Ruta predeterminada	Se configura una ruta IPv4 predeterminada para G0/0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0 Se configura una ruta IPv6 predeterminada para G0/0/0. R2(config)#ipv6 route ::/0 g0/0/0

Fuente. Propia

Paso 4: Configurar R3

Tabla 8. La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactiva la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada : class	R3(config)#enable secret class
Contraseña de acceso a la consola : cisco	R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)# login
Contraseña de acceso Telnet : cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifra las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado #
Interfaz S0/2/1	R3(config)#int s0/2/1 R3(config-if)#description conexion a R2

	R3(config-if)#ip address 172.16.2.1 255.255.255.252R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown Establece la descripción Establece la dirección IPv4. Se utiliza la siguiente dirección disponible en la subred. Establece la dirección IPv6. Según diagrama de topología para conocer la información de direcciones. Activa la interfaz
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.
Interfaz loopback 5	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.
Interfaz loopback 6	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 Establece la dirección IPv6. Usando el diagrama de topología para conocer la información de direcciones.
Ruta predeterminada	Se configura una ruta IPv4 predeterminada para s0/2/1. R3(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0 Se configura una ruta IPv6 predeterminada para s0/2/1. R3(config)#ipv6 route ::/0 g0/0/0

Fuente. Propia

Paso 5: Configurar S1

Tabla 9. La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactiva la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada : class	S1(config)#enable secret class
Contraseña de acceso a la consola : cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet : cisco	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifra las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado# S1(config)#exit

Fuente. Propia

Paso 6: Configurar el S3

Tabla 10. La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactiva la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada : class	S3(config)#enable secret class
Contraseña de acceso a la consola : cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet : cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit

Cifra las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado# S3(config)#exit

Fuente. Propia

Paso 7: Verificar la conectividad de la red
Utilice el comando ping para probar la conectividad entre los dispositivos de red.
Tabla 11. para verificar metódicamente la conectividad con cada dispositivo de red.

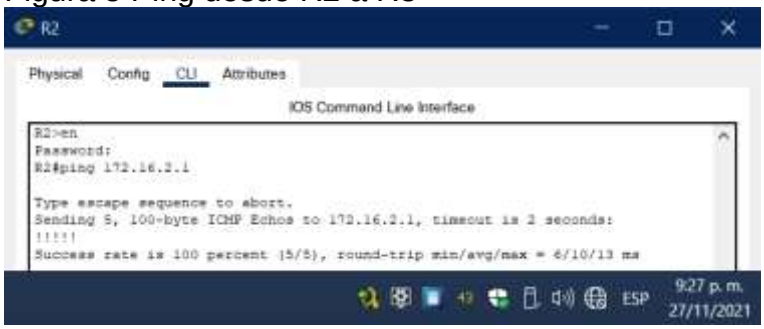
Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/2/0	172.16.1.2	Exitoso
R2	R3, S0/2/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.238	Exitoso

Fuente. Propia

Figura 4 Ping desde R1 a R2

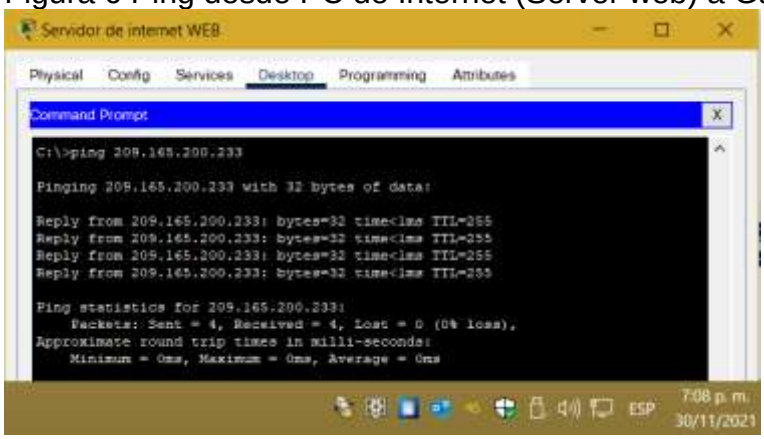
Fuente. Propia

Figura 5 Ping desde R2 a R3



Fuente. Propia

Figura 6 Ping desde PC de Internet (Server web) a Gateway predeterminado



Fuente. Propia

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN
Paso 1: Configurar S1
Tabla 12. La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crea la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit Se utiliza la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asigna la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit Asigna la dirección IPv4 a la VLAN de administración.

	Se utiliza la dirección IP asignada al S1 en el diagrama de topología
Asigna el Gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1 Asigna la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzá el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 Se utiliza la red VLAN 1 como VLAN nativa
Forzá el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 Se utilizar la red VLAN 1 como VLAN nativa
Configura el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access Se utilizar el comando interface range
Asigna F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport access vlan 21
Apaga todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente. Propia

Paso 2: Configurar el S3

Tabla 13. La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crea la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion exit Se utiliza la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asigna la dirección IP de administración	S1(config)#interface vlan 99

	S1(config-if)#ip address 192.168.99.3 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit Asigna la dirección IPv4 a la VLAN de administración. Utiliza la dirección IP asignada al S3 en el diagrama de topología
Asigna el Gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 Asigna la primera dirección IP en la subred como gateway predeterminado.
Forzá el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 Se utiliza la red VLAN 1 como VLAN nativa
Configura el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access Utilizar el comando interface range
Asigna F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apaga todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Fuente. Propia

Paso 3: Configurar R1

Tabla 14. Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configura la subinterfaz 802.1Q .21 en G0/0/1	R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 Descripción: LAN de Contabilidad Asigna la VLAN 21 Asigna la primera dirección disponible a esta interfaz

Configura la subinterfaz 802.1Q .23 en G0/0/1	R1(config)#int g0/1.23 R1(config-subif)#description LAN de Ing. R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Descripción: LAN de Ingeniería Asigna la VLAN 23 Asigna la primera dirección disponible a esta interfaz
Configura la subinterfaz 802.1Q .99 en G0/0/1	R1(config)#int g0/0/1.99 R1(config-subif)#description LAN de Admin R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Descripción: LAN de Administración Asigna la VLAN 99 Asigna la primera dirección disponible a esta interfaz
Activa la interfaz G0/0/1	R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown

Fuente. Propia

Paso 4: Verificar la conectividad de la red
Utilice el comando ping para probar la conectividad entre los switches y el R1.
Tabla 15. para verificar metódicamente la conectividad con cada dispositivo de red.

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Fuente. Propia

Figura 7 Desde S1 a R1 Vlan 99

Fuente. Propia

Figura 8 Desde S3 a R1 Vlan 99

Fuente. Propia

Figura 9 Desde S1 a R1 Vlan 21

Fuente. Propia

Figura 10 Desde S3 a R1 Vlan 23

Fuente. Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF
Paso 1: Configurar OSPF en el R1
Tabla 16. Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configura OSPF área 0	R1>enable R1#conf ter R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anuncia las redes conectadas directamente	R1(config-router)# network 192.168.99.1 0.0.0.0 area 0 R1(config-router)# network 192.168.23.1 0.0.0.0 area 0 R1(config-router)# network 192.168.21.1 0.0.0.0 area 0 R1(config-router)# network 172.16.1.1 0.0.0.3 area 0 Asigna todas las redes conectadas directamente.
Establece todas las interfaces LAN como pasivas	R1(config-router)# passive-interface g0/0/1.21 R1(config-router)# passive-interface g0/0/1.23 R1(config-router)# passive-interface g0/0/1.99

Fuente. Propia

Paso 2: Configurar OSPF en el R2
Tabla 17. La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Configura OSPF área 0	R2>enable R2#conf ter R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
Anuncia las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10. 0.0.0.0 area 0

Fuente. Propia

Paso 3: Configurar OSPF en el R3

Tabla 18. La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Configura OSPF área 0	R3>enable R3#conf ter R3(config)#router ospf 10 R3(config-router)#router-id 3.3.3.3
Anuncia redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.1 0.0.0.0 area 0 R3(config-router)#network 192.168.5.1 0.0.0.0 area 0 R3(config-router)#network 192.168.6.1 0.0.0.0 area 0
Establece todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6

Fuente. Propia

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera.

Tabla 19. Introduzca el comando de CLI adecuado para obtener la siguiente información:

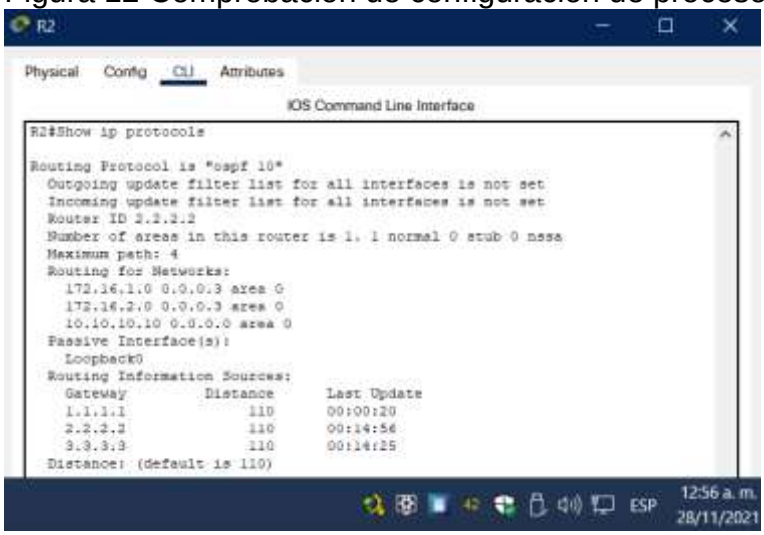
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Fuente. Propia

Figura 11 Comprobación de configuración de procesos OSPF en R1

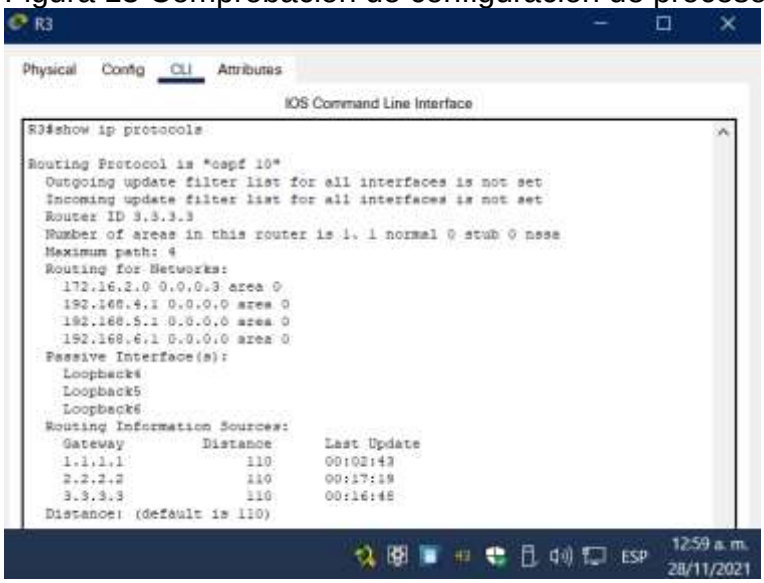
Fuente. Propia

Figura 12 Comprobación de configuración de procesos OSPF en R2



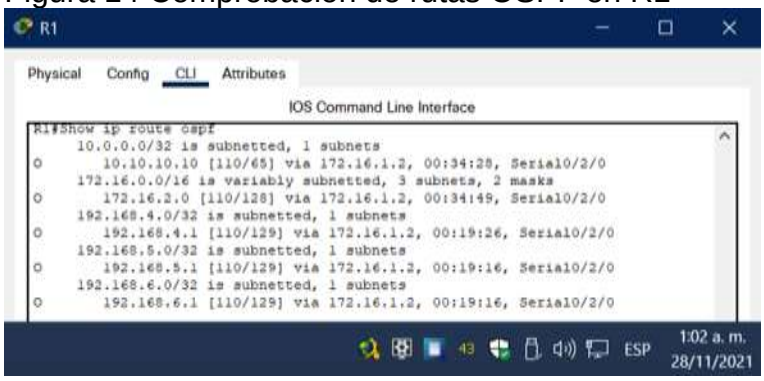
Fuente. Propia

Figura 13 Comprobación de configuración de procesos OSPF en R3



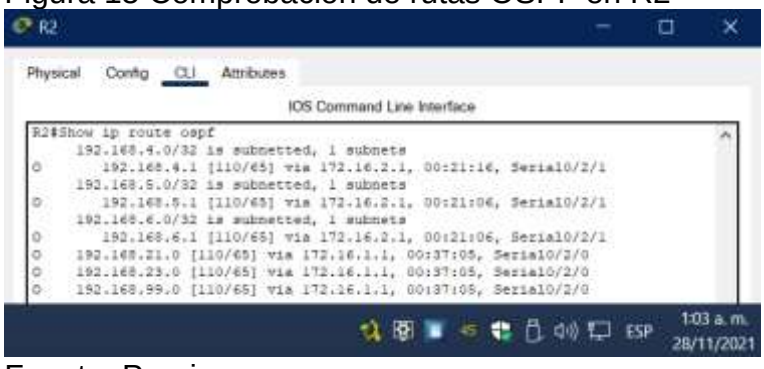
Fuente. Propia

Figura 14 Comprobación de rutas OSPF en R1



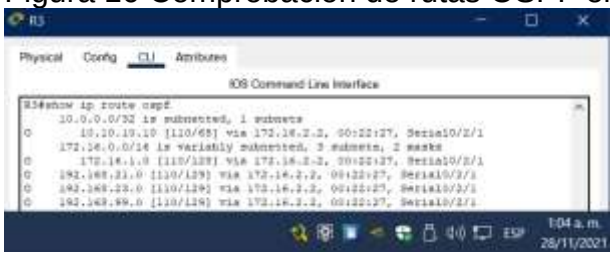
Fuente. Propia

Figura 15 Comprobación de rutas OSPF en R2



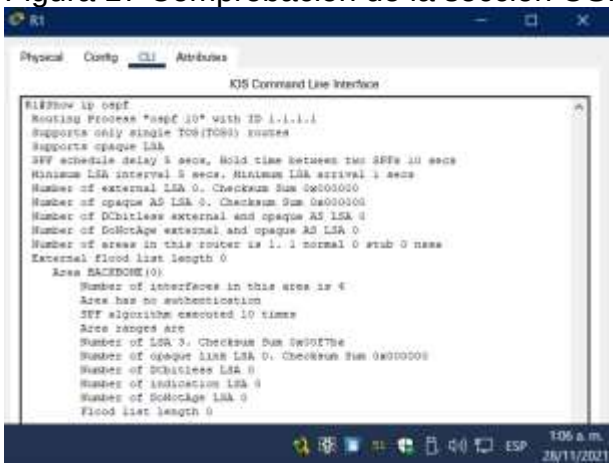
Fuente. Propia

Figura 16 Comprobación de rutas OSPF en R3



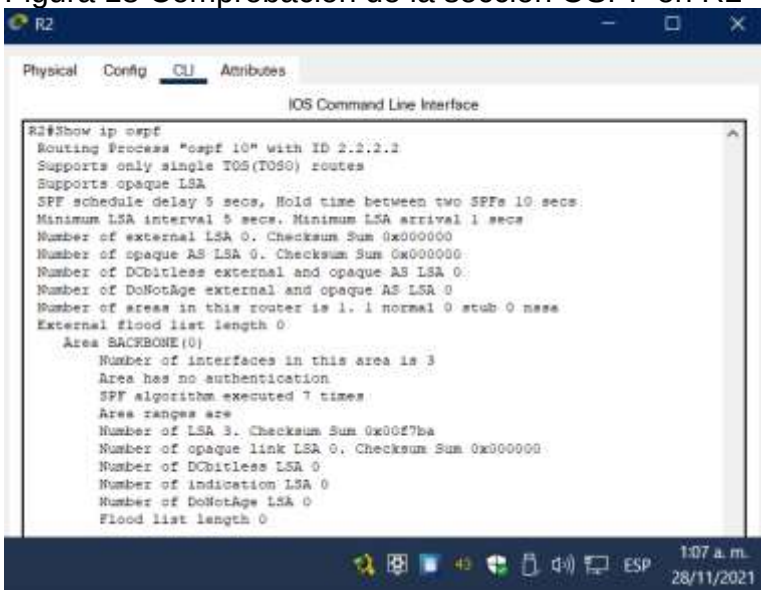
Fuente. Propia

Figura 17 Comprobación de la sección OSPF en R1



Fuente. Propia

Figura 18 Comprobación de la sección OSPF en R2



Fuente. Propia

Figura 19 Comprobación de la sección OSPF en R3

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

Tabla 20. Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Reserva las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>enable R1#conf ter R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reserva 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
Crea un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCTR1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crea un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR

	R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Fuente. Propia

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

Tabla 21. La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crea una base de datos local con una cuenta de usuario	R2>enable R2#conf ter R2(config)#username webuser privilege 15 secret cisco12345 Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilita el servicio del servidor HTTP	R2(config)#ip http server *Este comando es incompatible con pkt*
Configura el servidor HTTP para utiliza la base de datos local para la autenticación	R2(config)#ip http authentication local *Este comando es incompatible con pkt*
Crea una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 Dirección global interna: **209.165.200.229**
Asigna la interfaz interna y externa para la NAT estática	R2(config)#int g0/0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/2/0 R2(config-if)#ip nat inside R2(config-if)#int s0/2/1 R2(config-if)#ip nat inside R2(configif)#exit

Configura la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 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
Define el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.0 Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Define la traducción de NAT dinámic	R2(config)#ip nat inside source list 1 pool INTERNET

Fuente. Propia

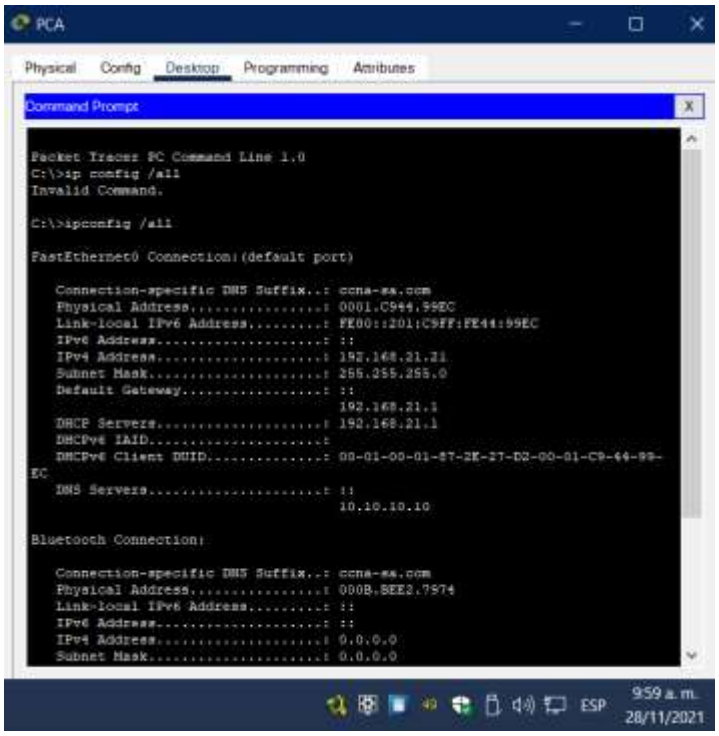
Paso 3: Verificar el protocolo DHCP y la NAT estática

Tabla 22. tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta.

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping ala PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

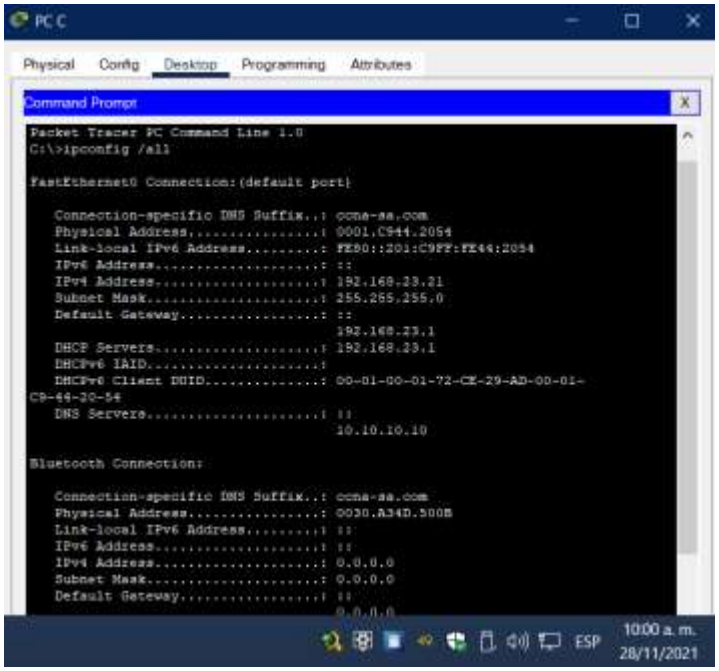
Fuente. Propia

Figura 20 Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



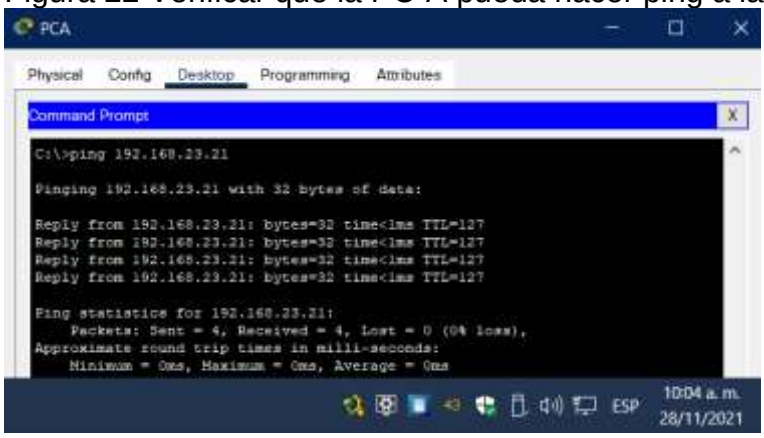
Fuente. Propia

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



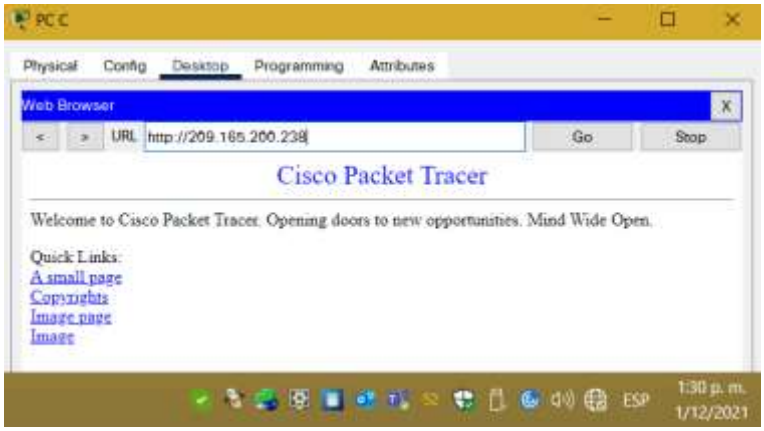
Fuente. Propia

Figura 22 Verificar que la PC-A pueda hacer ping a la PC-C



Fuente. Propia

Figura 23 Utilizar un navegador web en la computadora de Internet para acceder al servidor



Fuente. Propia

Parte 6: Configurar NTP

Tabla 23. Tareas parte 6, configurar NTP

Elemento o tarea de configuración	**Especificación**
Ajusta la fecha y hora en R2.	R2# clock set 9:00:00 5 March 2016 **5 de marzo de 2016, 9 a. m.**
Configura R2 como un maestro NTP.	R2(config)#ntp master 5 Nivel de estrato: **5**
Configura R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2 Servidor: **R2**

Configura R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifica la configuración de NTP en R1	R1#show ntp associations

Fuente. Propia

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

Tabla 24. Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	**Especificación**
Configura 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 R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit Nombre de la ACL: **ADMIN MGT**
Aplica la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet
Permite acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verifica que la ACL funcione como se espera	R1#telnet 172.16.1.2

Fuente. Propia

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

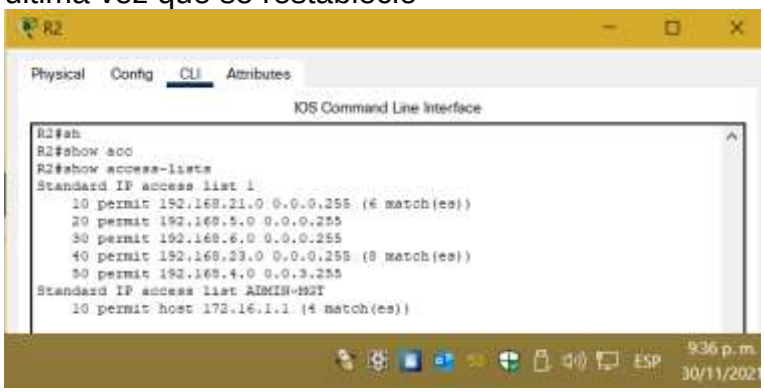
Tabla 25. Paso 2: Introducir el comando de CLI adecuado

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-list
Restablecer los contadores de una lista de acceso	R2#clear ip 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 s0/2/0
¿Con qué comando se muestran las traducciones NAT?	R2# show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se

	0agregarán 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

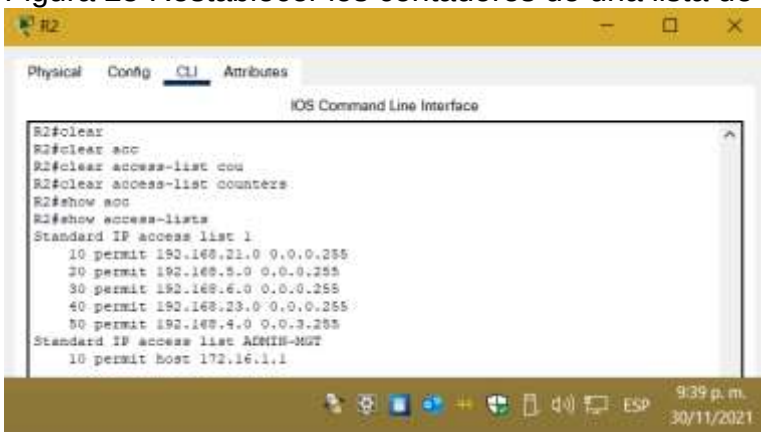
Fuente. Propia

Figura 24 Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció



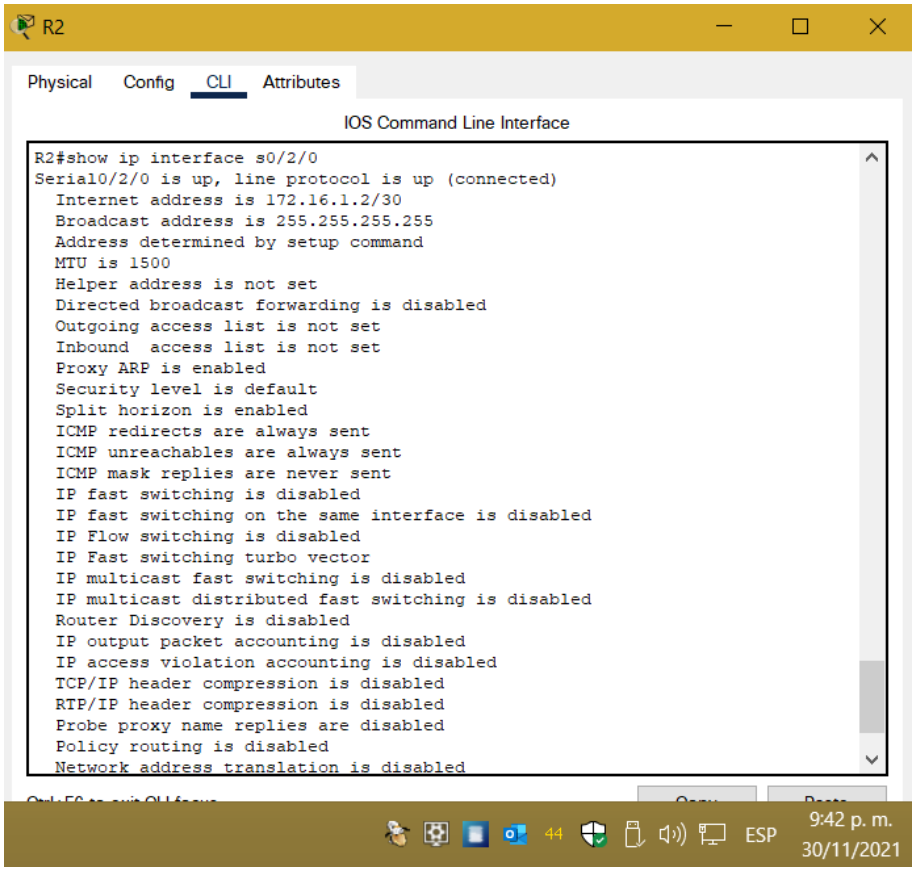
Fuente. Propia

Figura 25 Restablecer los contadores de una lista de acceso



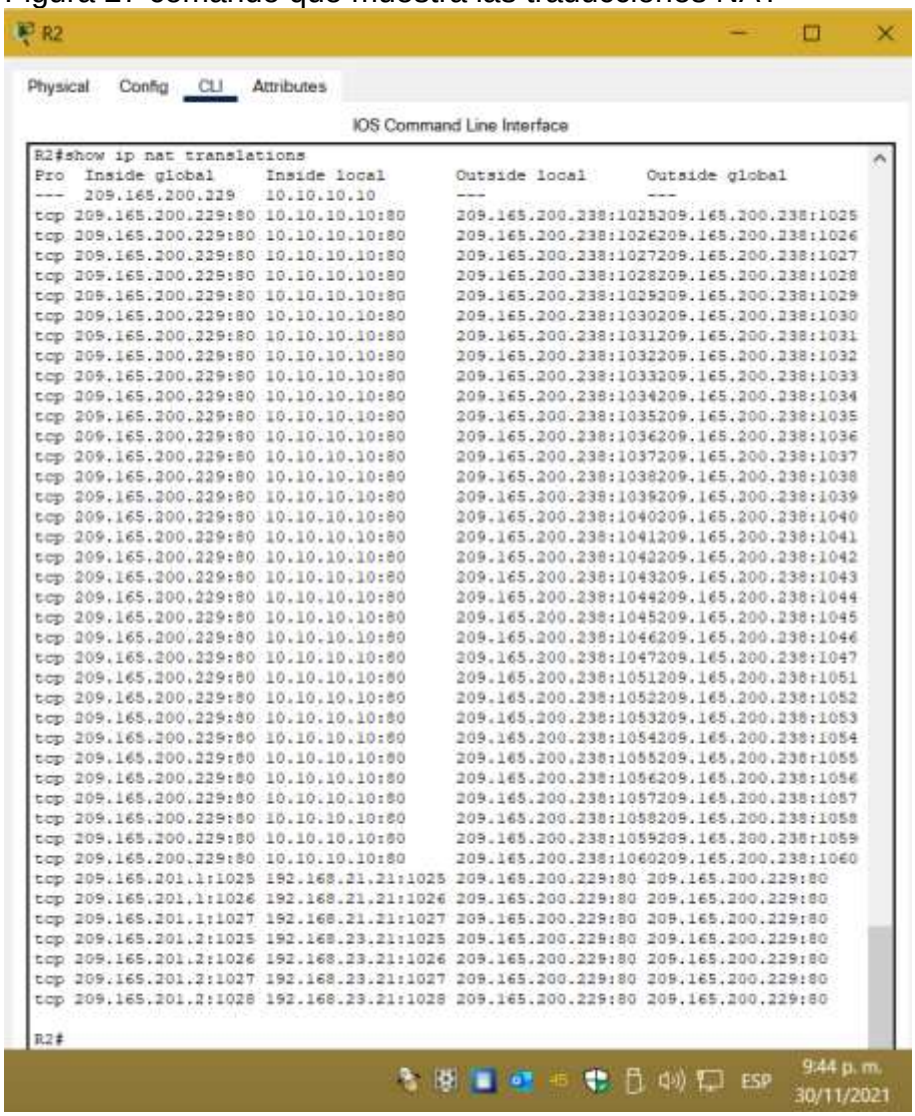
Fuente. Propia

Figura 26 comando que se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica



Fuente. Propia

Figura 27 comando que muestra las traducciones NAT



Fuente. Propia

CONCLUSIONES

En este trabajo logramos con éxito utilizar la modalidad “Proyecto Aplicado”, donde solventamos los problemas para los escenarios propuestos por la directora analizamos características y requerimientos específicos de cada uno, utilizamos herramientas de simulación y laboratorios de acceso remoto para establecer escenarios LAN/WAN que permitieron realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

Cumplimos los objetivos específicos que se propusieron con el desarrollo del escenario 1, así: Construimos la solución en el simulador la Red, desarrollamos el esquema de direccionamiento IP para las redes LAN, configuramos los aspectos básicos de los dispositivos de Red, configuramos los ajustes básicos de seguridad en un router y un switch, configuramos los hosts y verificamos la conectividad entre los equipos.

Alcanzamos los objetivos propuestos para el escenario 2, tales como: diseñar políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.
Asimismo, configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y las bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.
También, diseñar un esquema de direccionamiento IP para proporcionar conectividad; seguridad y acceso a la WAN mediante el uso del protocolo DHCP; listas de control de acceso y traducción de direcciones IP sobre NAT-PAT respectivamente.

BIBLIOGRAFÍA

[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] CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

[9] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

[10] CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

[11] CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

[12] CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

[13] CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

[14] CISCO. Principios básicos de routing y switching. Recuperado de: https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#6.1

[15] CISCO. Principios básicos de routing y switching . Recuperado de: https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#7.1.1.1