SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍAS CISCO

GUILLERMO ALONSO ARCHILA GUALDRON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA SISTEMAS

MALAGA

2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGÍAS CISCO

GUILLERMO ALONSO ARCHILA GUALDRON

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

DIRECTOR:

MSc. NANCY AMPARO GUACA GIRÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA SISTEMAS

MALAGA

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Málaga, Noviembre 30, de 2021

AGRADECIMIENTOS

Quiero agradecer a Dios primero que todo por haberme dado la salud y el entendimiento para poder lograr este gran reto de ser ingeniero de sistemas, a mis padres su apoyo incondicional en este proceso, a mi esposa que ha sido una base fuerte en todo momento para lograr superar cada obstáculo que se me presento durante mis estudios, a mis hijos que son esa sinergia en mi vida y cada día me dan la motivación para seguir a pesar de las adversidades, por último a mis docentes que se el esfuerzo que hacen para entregarnos un material de calidad y veraz para que podamos adquirir nuestras habilidades y así formar parte del engranaje económico y social de nuestra Colombia.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DNS: La sigla DNS proviene de la expresión inglesa Domain Name System: es decir, Sistema de Nombres de Dominio. Se trata de un método de denominación empleado para nombrar a los dispositivos que se conectan a una red a través del IP (Internet Protocol o Protocolo de Internet).

PREFIJO IP: Es una forma particular de expresar las direcciones de red y sus máscaras a partir de identificar solamente la cantidad de bits que se encuentran en uno en la máscara de subred.

MÁSCARA DE SUBRED: La máscara de subred es particularmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, y que es la que se encuentra referenciada en la tabla de enrutamiento.

PROTOCOLOS DE RED: Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

ROUTER: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

INTERFAZ: Se denomina interfaz a cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común. Se conoce como Interfaz Física a los medios utilizados para la conexión de un computador con el medio de transporte de la red.

RESUMEN

En la actividad desarrollada que se llamó “prueba de habilidades cisco ccna II 2021”, forma parte de las actividades establecidas dentro del Diplomado de Profundización CCNA, en el cual se estableció para identificar las competencias y habilidades que fueron adquiridas por los estudiantes a lo largo del diplomado. La idea era poner a prueba los conocimientos adquiridos en la solución de problemas propuestos en dos escenarios relacionados con el área de Networking.

En los dos escenarios se establecieron dos redes pequeñas; en el primer escenario se configuran un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts, además de configurar los parámetros necesarios para el correcto funcionamiento de cada uno de los dispositivos de red. En el segundo escenario se debe configurar una red pequeña con conectividad IPV4 e IPV6, seguridad de dispositivos, routing VLAN, OSPF dinámico, servido DHCP para asignación de direcciones IP a los equipos de cómputo.

Palabras Claves: cisco , vlan, ipv4, ipv6, routing, ospf, dhcp

ABSTRACT

In the activity developed called "CISCO CCNA II 2021 SKILLS TEST", it is part of the activities established within the ccna Deepening Diploma, in which it was established to identify the competencies and skills that were acquired by students throughout of the graduate. The idea was to test the knowledge acquired in solving problems proposed in two scenarios related to the Networking area.

In both scenarios, two small networks were established; In the first scenario, a router, a switch and equipment that support both IPv4 and IPv6 connectivity for the hosts are configured, in addition to configuring the necessary parameters for the correct operation of each of the network devices. In the second scenario, a small network must be configured with IPV4 and IPV6 connectivity, device security, VLAN routing, dynamic OSPF, DHCP server for assigning IP addresses to computer equipment.

Keywords: cisco, vlan, ipv4, ipv6, routing, ospf, dhcp

INTRODUCCION.

Esta actividad está diseñada en dos escenarios los cuales están acompañados de sus respectivos documentos para realizar cada uno de los procesos propuestos para la configuración de los dispositivos, el paso a paso de cada una de las etapas para solucionar para luego verificar la conectividad mediante el uso de los comandos de consola establecidos por el documento.

Revisando lo anterior el documento está formado por dos escenarios los cuales el estudiante podrá solucionar utilizando la herramienta Packet Tracer en las versiones 8 en adelante.

Al finalizar los dos escenarios propuestos debidamente documentados, este verificará el cumplimiento de la configuración de cada uno de los dispositivos de red establecidos en los escenarios, su funcionalidad, seguridad y conectividad de acuerdo con los parámetros establecidos en el presente documento.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

Topología

Figura 1 Topología escenario 1

Fuente. Autor.

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.

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

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 192.168.21.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. De direccionamiento base

Ítem	Requerimiento
Dirección de Red	192.168.21.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100 192.168.21.0/25
Requerimiento de host Subred LAN2	50 192.168.21.128/26
R1 G0/0/1	192.168.21.129/26

R1 G0/0/0	192.168.21.1/25
S1 SVI	192.168.21.2/25
PC-A	192.168.21.126/25
PC-B	192.168.21.190/26

Fuente. Autor.

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Tabla 2: Configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	**Especificación**
Desactivar la búsqueda DNS	# no ip domain-lookup 'Desactiva la búsqueda DNS'
Nombre del router	R1 #ho R1 ' Nombre del router R1'
Nombre de dominio	ccna-lab.com #ip domain-name ccna-lab.com ' dominio del router'
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass #enable secret ciscoenpass 'Configura la contraseña solicitada'
Contraseña de acceso a la consola	ciscoconpass R1(config-line)#password ciscoconpass ' Configuramos la contraseña de la consola'
Establecer la longitud mínima para las contraseñas	10 caracteres R1(config)#security passwords min-length 10 ' Con esta línea de comandos se establece la longitud máxima de caracteres para las contraseñas'
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** R1(config)#username admin password admin1pass 'Se establecen el nombre de usuario y la contraseña solicitada'

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#password ciscocisco R1(config-line)#login local 'Se realiza la correspondiente configuración vty para acceso loca con su correspondiente contraseña'
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh 'Se configura para que solo reciba acceso de SSH'
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption ' Se activa el cifrado de contraseñas de texto no cifrado'
Configure un MOTD Banner	R1(config)#banner motd #Este es el router de la Universidad Nacional Abierta y a Distancia UNAD, cualquier inclusion tendra efecto judiciales# ' Hemos configurado en Banner advertencia de forma personalizada'
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. R1(config)#int g0/0/0 R1(config-if)#ip address 192.168.21.129 255.255.255.192 R1(config-if)#description esta es la interfaz de la LAN 2 R1(config-if)#no shutdown 'Se establecieron los parámetros del reouter según las direcciones asignadas'
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. R1(config)#int g0/0/1 R1(config-if)#description Esta es la interfaz de la LAN uno R1(config-if)#ip address 192.168.21.1 255.255.255.128 R1(config-if)#no shutdow 'Se establecieron los parámetros del reouter según las direcciones asignadas'

Generar una clave de cifrado RSA	Módulo de 1024 bits 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 'De esta forma le hemos especificado el nivel de encriptación a 1024'

Fuente. Autor.

Tabla 3. Configuración de S1.

Tarea	**Especificación**
Desactivar la búsqueda DNS.	# no ip domain-lookup 'Desactiva la búsqueda DNS'
Nombre del switch	**S1** #ho S1 ' Nombre del SW R1'
Nombre de dominio	**ccna-lab.com** ccna-lab.com #ip domain-name ccna-lab.com 'dominio del SW'
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** ciscoenpass #enable secret ciscoenpass 'Configura la contraseña solicitada'
Tarea	**Especificación**
Contraseña de acceso a la consola	**ciscoconpass** ciscoconpass S1(config-line)#password ciscoconpass ' Configuramos la contraseña de la consola'
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** S1(config)#username admin password adminpass1 ' Se establece usuario y

	contraseña del administrador del dispositivo’
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#password ciscocisco S1(config-line)#login local ‘Se establece las líneas de comando para establecer inicio de sesión’
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit ‘Se han establecido las conexiones tipo SSH’
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption ‘Se activa el cifrado de contraseñas’
Configurar un MOTD Banner	S1(config)#banner motd #Este el SW de la UNAD, por favor no entrar aqui# ‘Se configura el banner MOTD del SW’
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa The name for the keys will be: S1.ccn-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] ‘La clave de cifrado se ha generado y se ha actualizado a 1024’
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento S1(config)#int vlan1 *Mar 1 2:23:23.345: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip add S1(config-if)#ip address 192.168.21.2 255.255.255.128 S1(config-if)#no sh S1(config-if)#no shutdown

	‘Líneas de comando para establecer dirección IP y mascara de red. Se aplican los cambios’
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. S1(config)#ip default-gateway 192.168.21.1 ‘Se configura las puesta de enlace predeterminada’

Fuente. Autor.

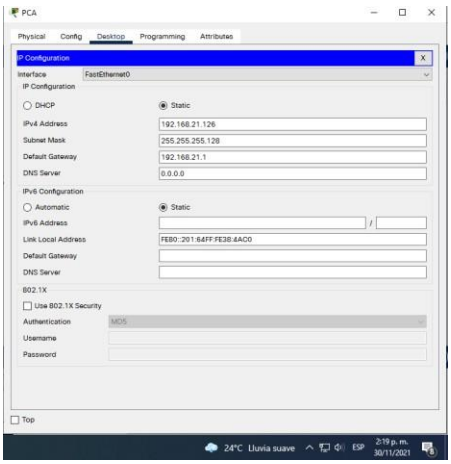
Paso 2. Configurar los equipos

Tabla 4. Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

PC-A Network Configuration	
Descripción	
Dirección física	0001.6438.4AC0
Dirección IP	192.168.21.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.21.1

Fuente. Autor.

Figura 2. Configuración PC-A



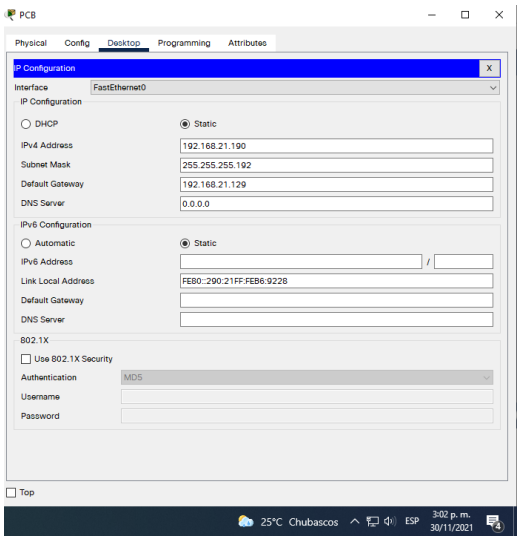
Fuente. Propia

Tabla 5. Configuración PC-B

PC-B Network Configuration	
Descripción	
Dirección física	0090.21B6.9228
Dirección IP	192.168.21.190
Máscara de subred	255.255.255.192
PC-B Network Configuration	
Gateway predeterminado	192.168.21.1

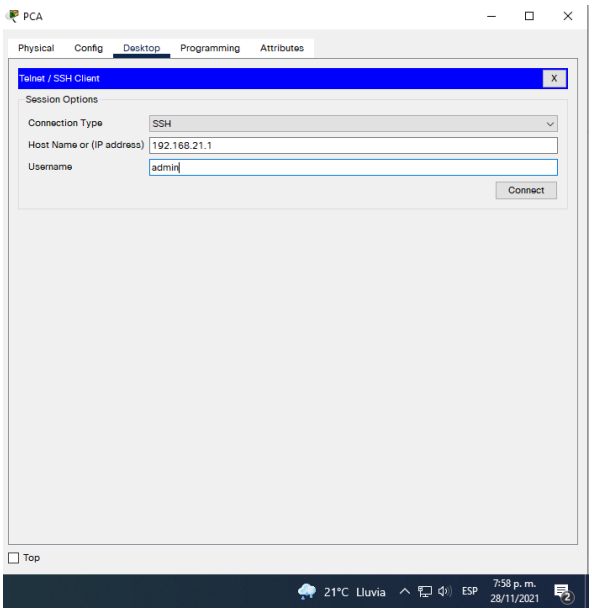
Funte. Propia

Figura 3. Configuración PC-B



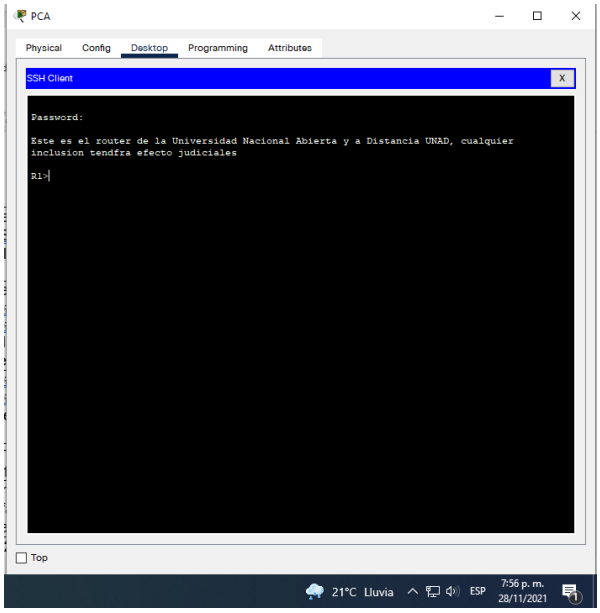
Fuente. Propia.

Figura 1 Validación usuario SSH desde PCA



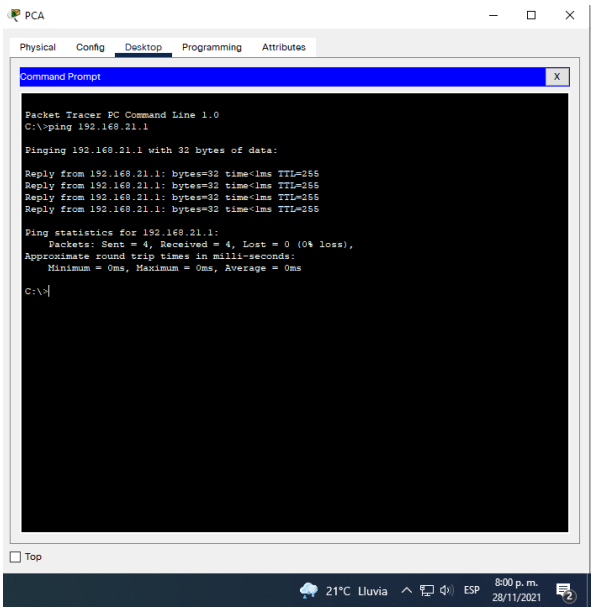
Fuente: Propia.

Figura 2. Validación SSH



Fuente: Propia.

Figura 3 Verificación con puerta de enlace predeterminada a través de PING



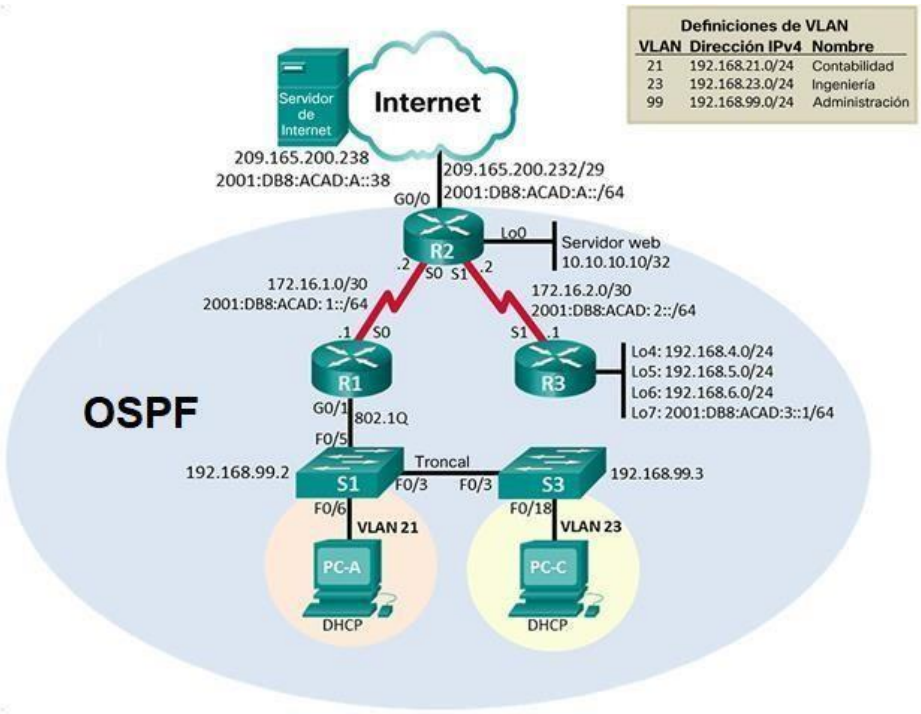
Fuente: Propia.

Escenario 2

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

Topología

Figura 4 Topología escenario 2



Fuente: Autor.

Tabla 6: 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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Router#

Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash: Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#

Fuente. Propia.

Tabla 7. Configurar la computadora de Internet.

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

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:2::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente. Autor

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Tabla 8. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/2/0	R1(config)#interface serial 0/2/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 R1(config)#ipv6 route ::/0 s0/2/0 R1(config)#ipv6 unicast-routing

Fuente. Autor.

Nota: Todavía no configure G0/1.

Tabla 9. Configurar R2.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http secure-server
Mensaje MOTD	R2(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/2/0	R2(config)#interface serial 0/2/0 R2(config-if)#description R1 a R2 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit

Interfaz S0/2/1	R2(config)#interface serial 0/2/1 R2(config-if)#description R2 a 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 R2(config-if)#exi
Interfaz G0/0 (simulación de Internet)	R2(config)#interface gigabitEthernet 0/0/0 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0/0 R2(config)#.

Fuente. Autor.

Tabla 10. Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup

Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohibe el acceso no autorizado#
Interfaz S0/2/1	R3(config)#interface serial 0/2/1 R3(config-if)#description R3 a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)# R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#
Rutas predeterminadas	

Fuente. Autor.

Tabla 11. Configurar S1

La configuración del S1 incluye las siguientes tareas:

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

Fuente. Autor.

Tabla 12. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohibe el acceso no autorizado#.

Fuente. Autor.

Paso 7:

Tabla 13. Verificar la conectividad de la red.

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100

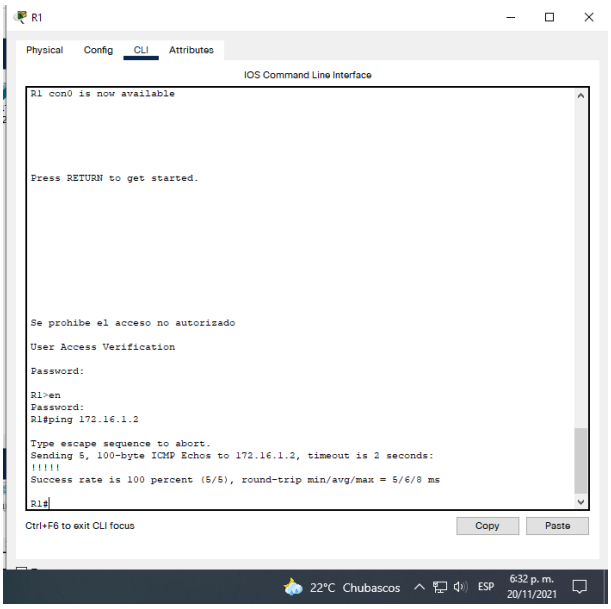
			percent (5/5), roundtrip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), roundtrip min/avg/max = 5/6/10 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Packet Tracert SERVER Command Line 1.0 C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233:

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

Fuente. Autor.

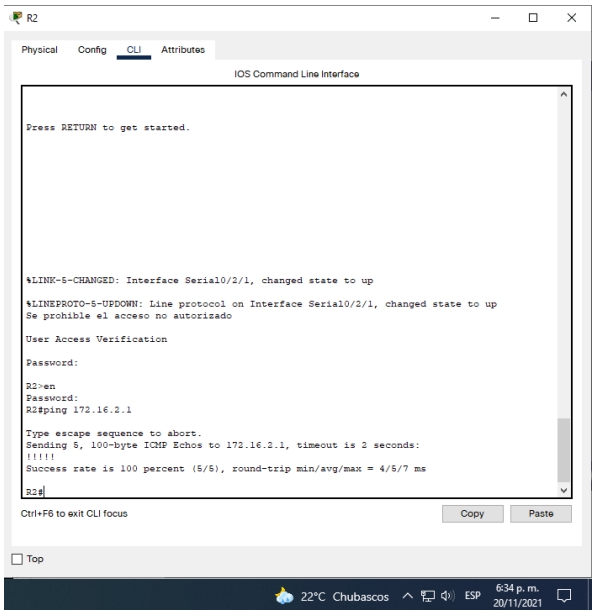
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 6 Ping de R1 a R2.



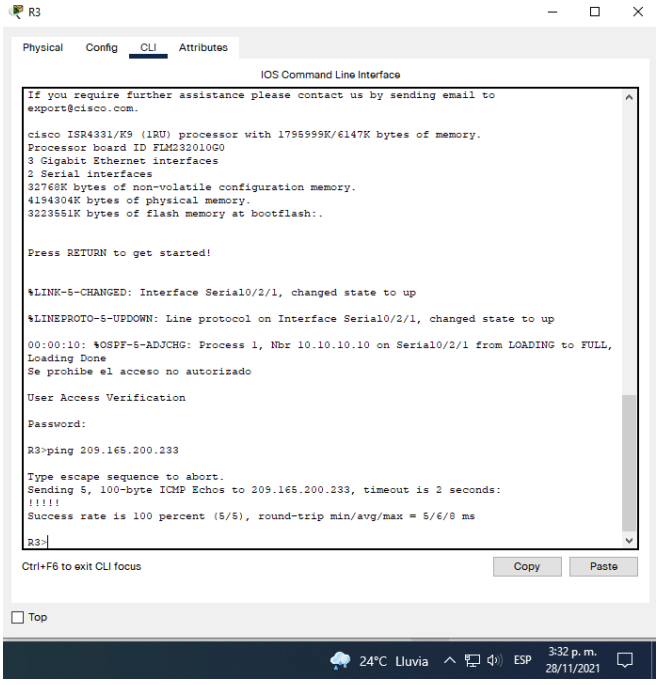
Fuente: Propia.

Figura 7 Ping de R2 a R3.



Fuente: Propia.

Figura 8 Ping de PC de Internet a Gateway predeterminado



Fuente: Propia.

Tabla 14. Configurar el S1 VLAN Administración

Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear 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
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)# S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access

	S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Fuente. Autor.

Tabla 15 Configurar el S3 VLAN Administración

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#interface fastEthernet 0/3 S3(config-if)# S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

	S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Fuente. Autor.

Tabla 16 Configurar R1 VLAN Administración

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface gigabitEthernet 0/0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#interface gigabitEthernet 0/0/1.23 R1(config-subif)#description accounting LAN de Ingenieria

	R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#interface gigabitEthernet 0/0/1.99 R1(config-subif)#description accounting LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown R1(config-if)#exit

Tabla 17 Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

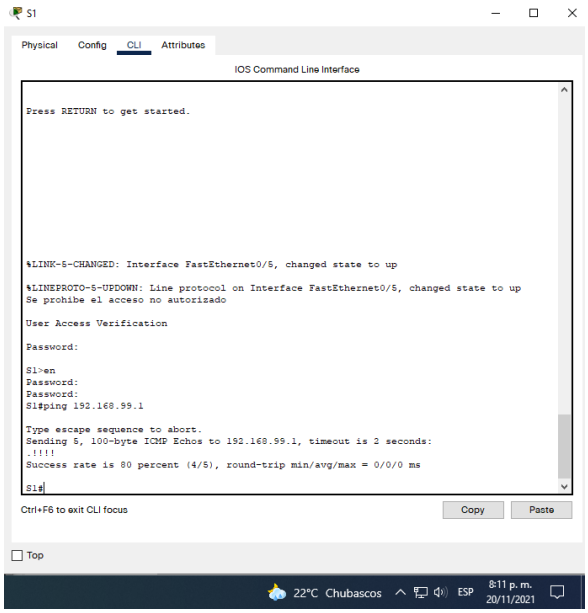
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2

			seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.99.1, 57 timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#

S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms 58 S3#

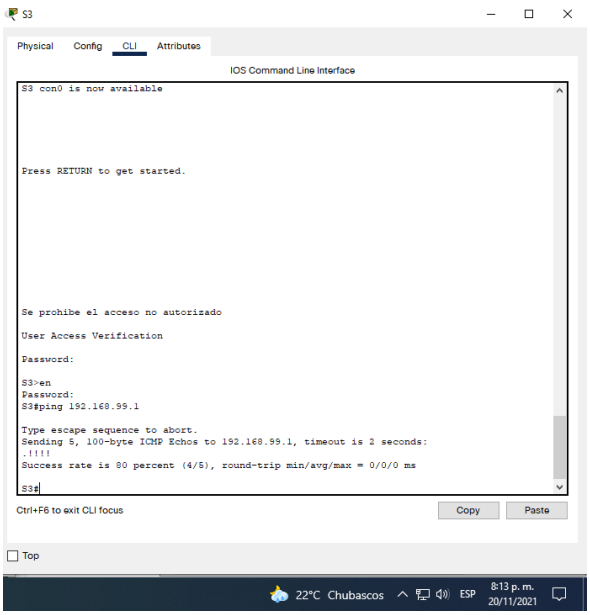
Fuente. Autor.

Figura 9 Ping S1 a VLAN Administración



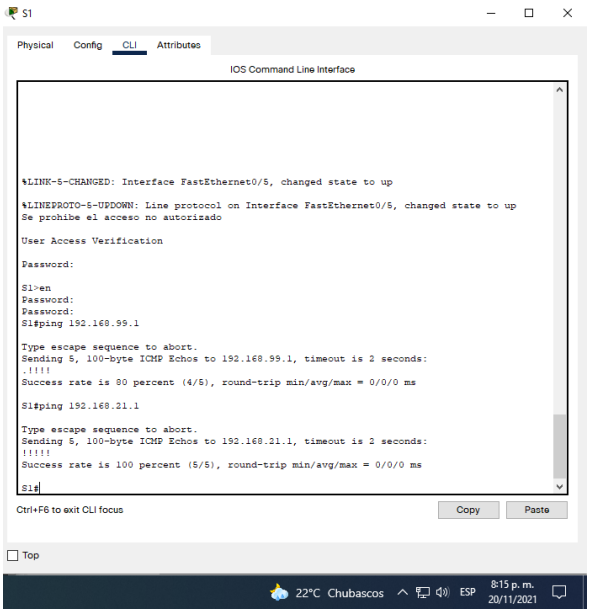
Fuente: Propia

Figura 10 Ping S3 a VLAN Administración



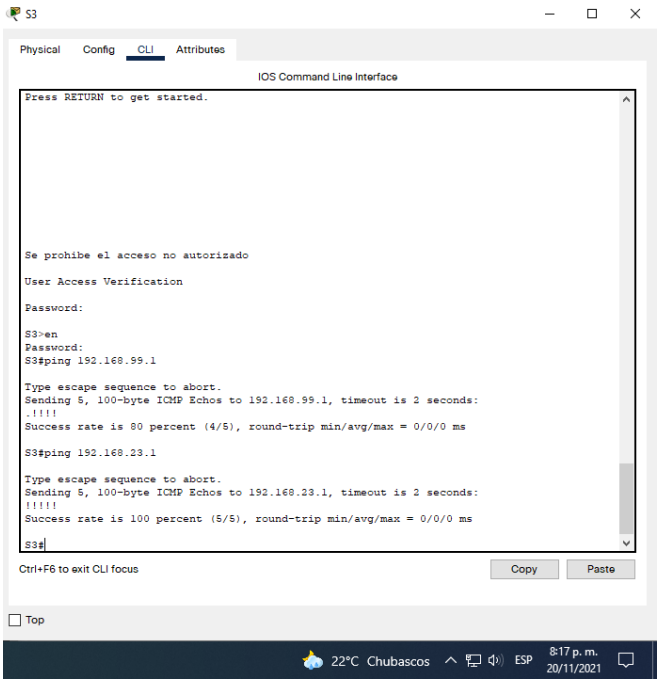
Fuente: Propia.

Figura 11 Ping de S1 a VLAN 21



Fuente: Propia.

Figura 12. Ping de S3 a la VLAN 23



Fuente: Propia.

Tabla 18 Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network

	192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passiveinterface gi0/1.21 R1(config-router)#passiveinterface gi0/1.23 R1(config-router)#passiveinterface gi0/1.9
Desactive la sumarización automática	

Fuente. Autor.

Tabla 19 Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar 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 209.165.200.232 0.0.0.7 area 0 Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	

Fuente. Autor.

Tabla 20. Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	

Fuente. Autor.

Tabla 21. Verificar la información de OSPF

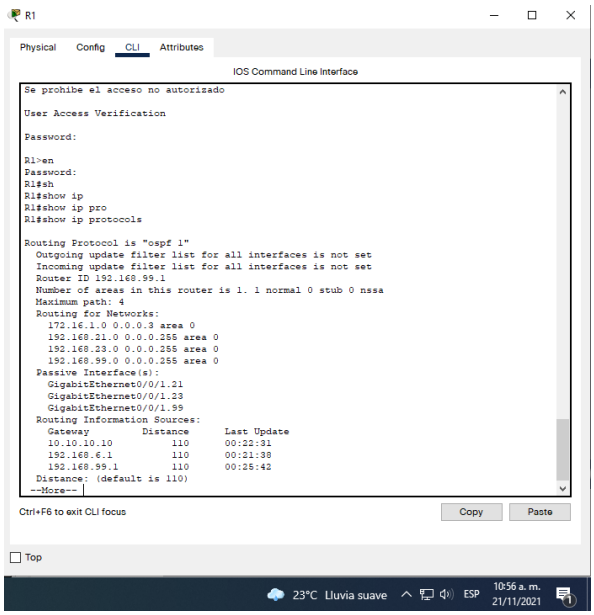
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

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 database

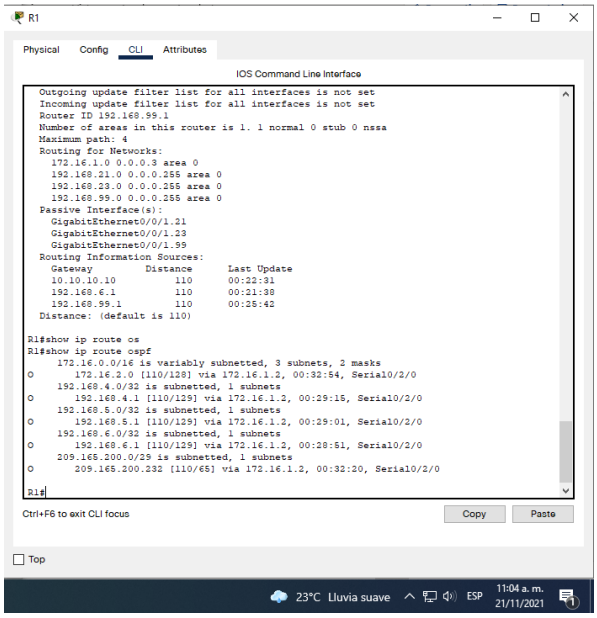
Fuente. Autor.

Figura 13. Comando para ver ID del proceso OSPF



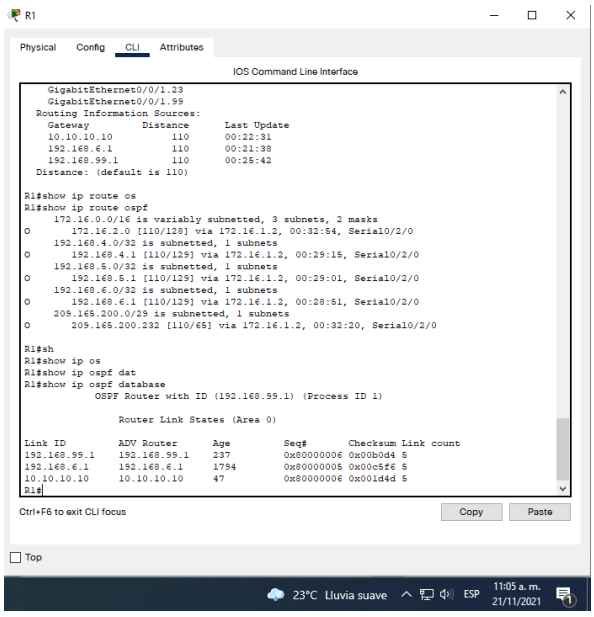
Fuente: Propia.

Figura 14 Comando para mostrar solo las rutas OSPF



Fuente: Propia.

Figura 15. Muestra la sección de OSPF de la configuración en ejecución



Fuente: Propia.

Tabla 22 Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Fuente. Autor.

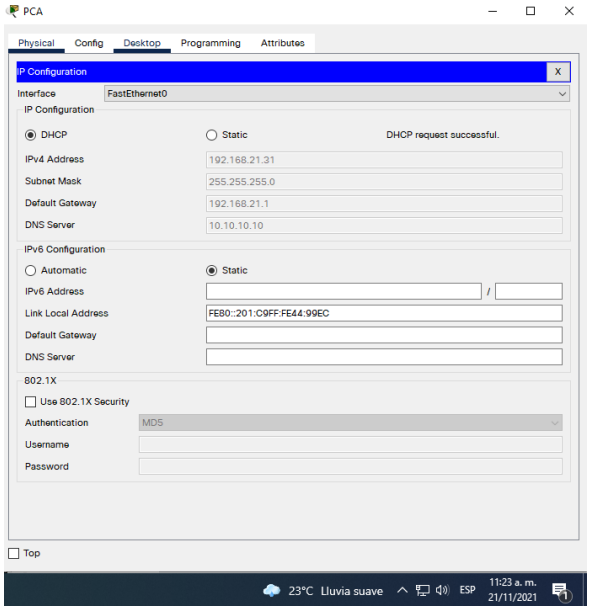
Tabla 23: Configurar la NAT estática y dinámica en el R2 La configuración del R2 incluye las siguientes tareas:

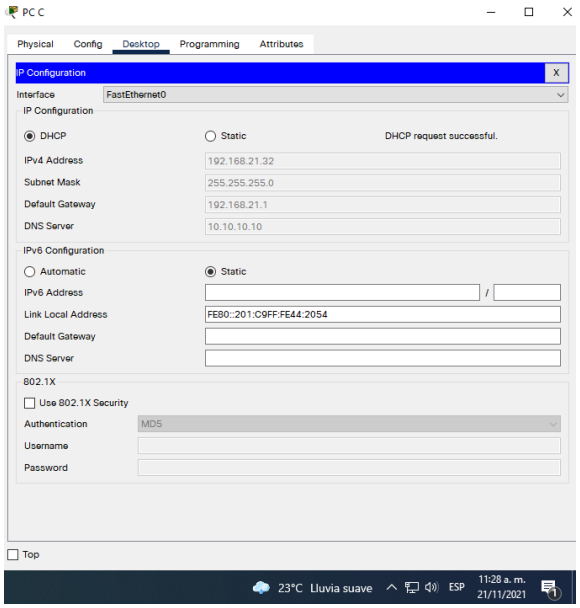
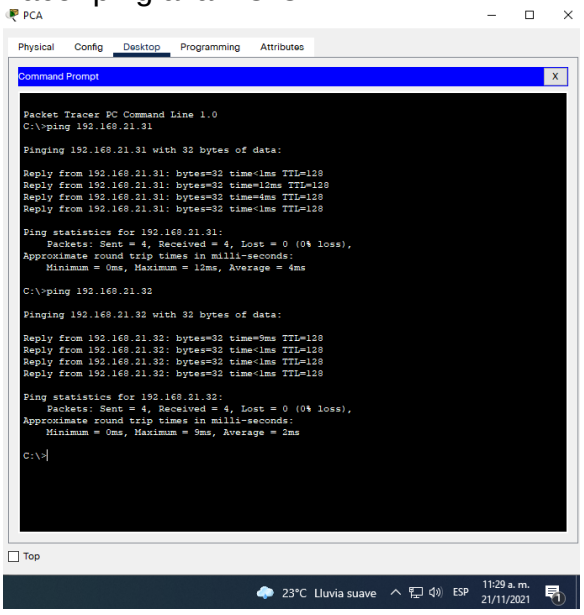
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0 R2(config-if)#ip nat inside
Configurar 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 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNE

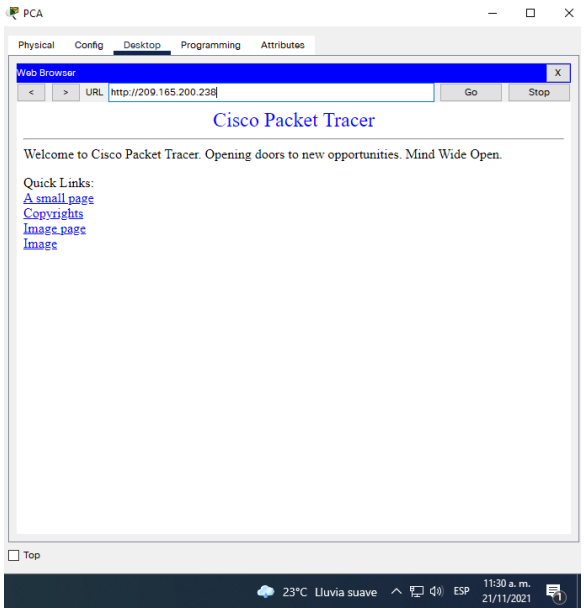
Fuente. Autor

Tabla 24. Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 16 Verificar que la PC-A haya adquirido información de IP del servidor de DHCP  Fuente: Propia.

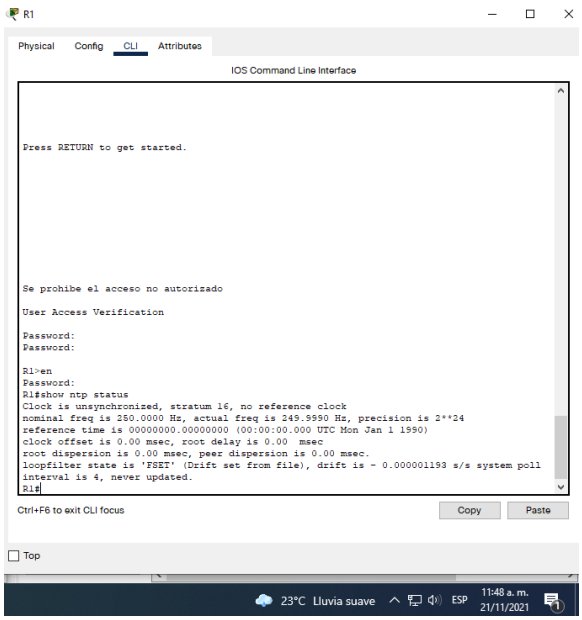
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 17 Verificar que la PC-C haya adquirido información de IP del servidor de DHCP  Fuente: Propia.
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 18 Verificar que la PC-A pueda hacer ping a la PC-C.  Fuente: Propia.

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**	Figura 19 navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238).  Fuente: Propia.

Fuente Autor.

Tabla 25. Configurar NTP

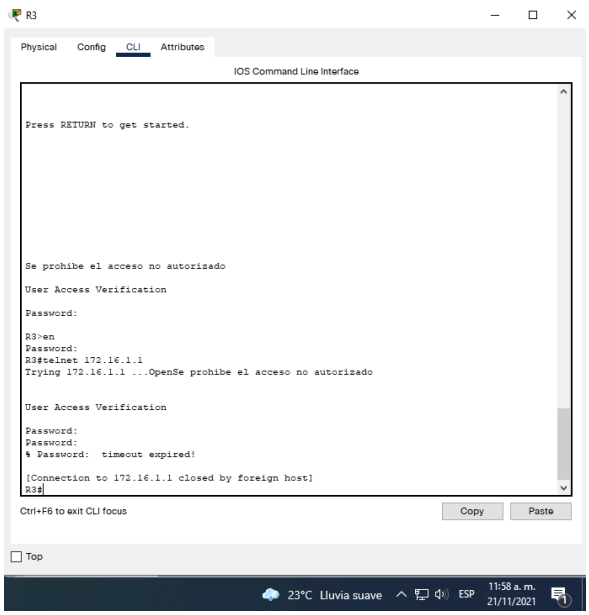
Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 6 Mar 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp updatecalendar
Verifique la configuración de NTP en R1.	

	Figura 20 Verifique la configuración de NTP en R1.  Fuente: Propia.

Fuente. Autor.

Tabla 26. Configurar y verificar las listas de control de acceso (ACL) Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip accesslist standard ADMINMGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-stdnacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#acces R2(config-line)#accessclass ADMIN-MGT in R2(config-line)#exit

Verificar que la ACL funcione como se espera	Figura 21 Verificación del funcionamiento de la ACL  Fuente: Propia.

Fuente. Autor.

Tabla 27. Introducir el comando de CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2(config)#show access-list

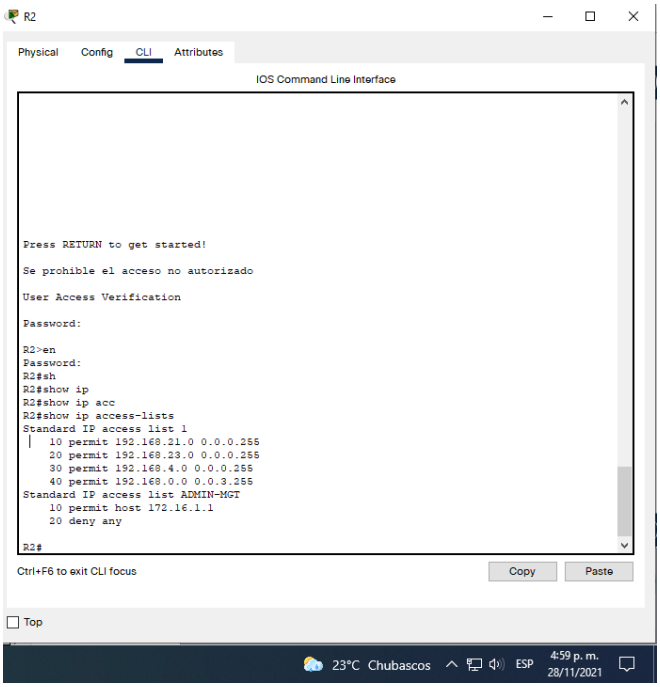
	Figura 22 Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció.  Fuente: Propia.
Restablecer los contadores de una lista de acceso	R2(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2 (config)#show interfaces

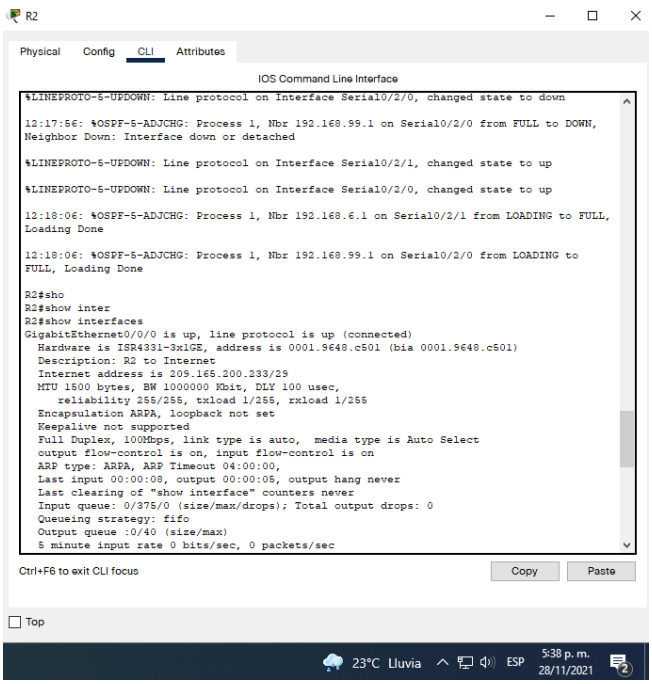
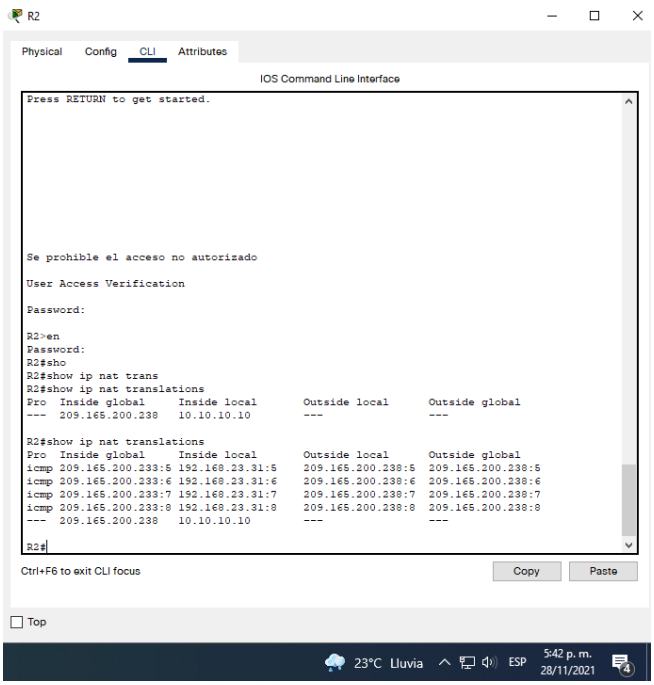
	Figura 23 Comando para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica  Fuente: Propia.
¿Con qué comando se muestran las traducciones NAT?	R2 (config)#show ip nat translations

	Figura 24 Visualización del uso del comando show ip nat translations  Fuente: Propia: **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

Fuente. Autor.

CONCLUSIONES

En el diplomado de profundización se adquirieron las bases necesarias para dar solución a nivel de Networking en la vida cotidiana configurando diferentes dispositivos de red para poder hacer buen uso de los datos y poder garantizar la seguridad y la integralidad de la estructura de red de la organización.

Se identificaron los diferentes dispositivos de red y su configuración basándose en los parámetros establecidos por el fabricante y las políticas de seguridad establecidas por la organización.

Durante el diplomado se identifica la herramienta Packet Tracert para el desarrollo de las actividades propuestas en los diferentes escenarios de implementación de redes tipo LAN, WAN, lo cual nos permitió realizar análisis sobre el comportamiento y enrutamiento de los datos.

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.

VESGA-FERREIRA, Juan Carlos; GRANADOS-ACUNA, Gerardo and VESGA-BARRERA, José Antonio. Evaluation of the performance of a network LAN over Powerline Communications for the transmission of VoIP. Iteckne [online]. 2016, vol.13, n.1, pp.83-95. ISSN 1692-1798.

Vesga Ferreira, Juan Carlos [1] ; Granados Acuña, Gerardo [2]
[1] Pontifical Bolivarian University
[2] Esp. en Telecomunicaciones. ECBTI – UNAD

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado dehttps://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1