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

JHON FREDY ORTEGA BURBANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
IBAGUE (TOLIMA)
2021

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

JHON FREDY ORTEGA BURBANO

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

DIRECTOR:

MSC. RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

IBAGUE, TOLIMA

2021

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

IBAGUE, TOLIMA 23 de noviembre de 2021

AGRADECIMIENTOS

En primer lugar, agradezco a dios por la vida y por permitirme aprovechar cada una de las experiencias existidas en este arduo camino educativo.

Así mismo agradezco a todas las personas que apoyaron mi proceso académico, quienes con sus apalabras de apoyo y motivación, me impulsaron a cumplir este sueño que se ve reflejado en la formación profesional y personal.

Muestro mi gratitud a mi tutor de proyecto, magister don Raúl Bareño Gutiérrez quien, con su conocimiento, paciencia y dedicación, me apoyo de manera significativa en cada una de las fases del del diplomado.

Así, agradezco infinitamente a mi madre y a mi padre por darme la vida, por ser esa base fundamental que desde mi infancia me apoyaron a culminar las etapas personales y educativas, gracias por su paciencia, por su amor y comprensión.

De la misma manera agradezco a mi hermana y por sus consejos y apoyo continuo que medio para continuar con mi carrera.

Finalmente, a mis compañeros, quienes me brindaron con generosidad sus conocimientos, con los que establecimos comunicación para fortalecer nuestra amistad y conocimientos, gracias por compartir momentos de alegría y tristeza, me ayudaron a que hoy seamos una familia.

Por último, quiero agradezco a la Universidad Nacional Abierta y a Distancia, por brindarme la oportunidad de culminar mis estudios en esta grandiosa universidad, que me brindo su confianza, su metodología y sus docentes que vieron por crecer juntos en este proyecto.

¡Muchas gracias por todo!

CONTENIDO

AGRADECIMIENTOS 4
CONTENIDO 5
LISTA DE TABLAS 7
LISTA DE FIGURAS 8
GLOSARIO 9
RESUMEN 11
ABSTRACT 11
INTRODUCCIÓN 12
DESARROLLO 13
1. Escenario 1 13
Paso 1. Topología escenario 1 13
Paso 2. Simulación de escenario 1en Packet Tracer. 13
Paso 3. Direccionamiento ip 14
Paso 4. Configuración básica del R1 15
Paso 6. Configuración básica del S1 17
Paso 8. Información de configuración del PC-A 18
Paso 9. Información de configuración del PC-B 20
Paso 10. Evidencias de pruebas de ping desde al PC-A a PC-B y viseversa. 22
2. Escenario 2 25
Paso 1. Simulación de escenario 2 en Packet Tracer. 26
Paso 1: Inicializar y volver a cargar los routers y los switches 26
Parte 2:Configurar los parámetros básicos de los dispositivos 27
Paso 2: Configurar la computadora de Internet 27
Paso 3: Configurar R1 27
Paso 4: Configurar R2 28
Paso 5: Configurar R3 30
Paso 6: Configurar S1 32
Paso 7: Configurar el S3 32
Paso 8: Verificar la conectividad de la red 33

Paso 9: Configurar S1 35
Paso 10: Configurar el S3 36
Paso 11: Configurar R1 37
Paso 12: Verificar la conectividad de la red 38
Paso 13: Configurar OSPF en el R1 41
Paso 14: Configurar OSPF en el R2 41
Paso 15: Configurar OSPFv6 en el R3 42
Paso 19: Verificar el protocolo DHCP y la NAT estática 46
Paso 20: Restringir el acceso a las líneas VTY en el R2 48
Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 49
CONCLUSIONES 51
BIBLIOGRÁFIA 52

LISTA DE TABLAS

Tabla 1. Direccionamiento ip 14
Tabla 2. Documentación de configuración R1 15
Tabla 3. Documentación de configuración S1 17
Tabla 4. Información de configuración del PC-A 18
Tabla 5. Información de configuración del PC-B 20
Tabla 6. Comandos para Inicializar a cargar los dispositivos. 26
Tabla 7. Configuración de parámetros básicos 27
Tabla 8. Configuración de R1 27
Tabla 9. Configuracion R2 28
Tabla 10. Configuración R3 30
Tabla 11. Configuración S1 32
Tabla 12. Configuración del S3 32
Tabla 13. Pruebas de conectividad 33
Tabla 14. Configuración de la seguridad, vlan en el switch s1 35
Tabla 15. Configuración seguridad, vlan en el S3 36
Tabla 16. Configuración R1 37
Tabla 17. conectividad de la red 38
Tabla 18. Configuración OSPF en el R1 41
Tabla 19. Configuración OSPF en el R2 41
Tabla 20. Configuración OSPFv6 en el R3 42
Tabla 21.comandos para verificar la información de OSPF 43
Tabla 22. Configuración el R1 como servidor de DHCP 44
Tabla 23. Configurar la NAT estática y dinámica en el R2 45
Tabla 24. Comandos para verificar el protocolo DHCP y la NAT estática 46
Tabla 25. Configuración de NTP 47
Tabla 26. Configuración de (ACL) 48
Tabla 27. Comandos de CLI 49

LISTA DE FIGURAS

Figura 1. Topología escenario 1 13
Figura 2. Simulación de escenario 1en Packet Tracer. 13
Figura 3. Configuración física del PC-A 19
Figura 4. Configuración básica del PC-B 21
Figura 5. Evidencia de ping desde al PC-A a PC-B 22
Figura 6. Evidencia de ping desde al PC-B a PC-A 23
Figura 7. Topología escenario 2 25
Figura 8. escenario 2 en Packet Tracer 26
Figura 9. conectividad de la red por medio del comando ping 34
Figura 10. Pruebas de conectividad entre el S1 y el R1 40
Figura 11. Pruebas de conectividad entre el S3 y el R1 40
Figura 12. información de OSPF comando show 43
Figura 13. Evidencias de configuraciones de DHCP y NAT estática 46

GLOSARIO.

Direccionamiento IP: El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Router: Un Router es útil para dividir las LAN en dominios de difusión (broadcast) separados, sobre todo se debe utilizar al conectar estas LAN sobre una WAN. Los Routers se comunican entre sí mediante conexiones WAN, y conectan redes dentro de sistemas locales, así como el backbone de Internet.

Enlace serial: Las comunicaciones a través de una conexión serial son un método de transmisión de datos en el que los bits se transmiten en forma secuencial por un único canal. Los puertos serie son bidireccionales y a menudo se los denomina «puertos bidireccionales» o «puertos de comunicaciones».

Switch: Un switch o conmutador 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 (o técnicamente IEEE 802.3).

Modelo OSI: El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como “modelo OSI”, (en inglés, Open System Interconnection) es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization).1 Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar.2 Su desarrollo comenzó en 1977.

Dirección MAC: Una dirección MAC es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular. Una dirección MAC consiste en seis grupos de dos caracteres, cada uno de ellos separado por dos puntos.

Modelo TCP/IP: es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet. A veces se denomina como ', “modelo DoD” o “modelo DARPA”. Es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo

los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

Red LAN: Local Área Network) Red de Área Local. Como su nombre indica, es una red de ordenadores de tamaño pequeño/medio localizada en un edificio (como máximo). Se conectan los ordenadores a través de tarjetas de red, y las arquitecturas más conocidas son Ethernet y Token-Ring

Protocolo: El protocolo es la parte software de la red. Se encarga básicamente de establecer las reglas de comunicación entre equipos de la red, definir el formato de las informaciones que circulan por la red y también debe habilitar mecanismos para permitir la identificación de los equipos en la red.

Topología de red: es él termino técnico que se utiliza para describir la disposición física en la que está configurada una red.

Subnetting: La técnica del subnetting consiste en dividir las redes en distintas redes más pequeñas o subredes. De esta forma un administrador informático o de red puede dividir la red interna de un gran edificio en subredes más pequeñas

Cableado: El cable es el medio que los PC de una red se pueden comunicar el uno con el otro. Hay distintos tipos de cables para hacer una red, que siempre está sujeto a la topología de la red, con esto deberemos tener en cuenta varios factores.

Ethernet: Ethernet es un estándar de redes de área local para computadoras, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones. Su nombre procede del concepto físico de éter.

Capa de red: El nivel de red o capa de red, según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Cisco Systems: es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

VLAN: una red de área local virtual (VLAN) es una red conmutada que está segmentada lógicamente por función, área o aplicación, sin tener en cuenta las ubicaciones físicas de los usuarios.

RESUMEN

En el desarrollo del presente proyecto se abordará las temáticas de administración, configuración y diseño de redes escalables. es así como el diplomado de profundización CCNA CISCO (LAN/WAN), permite tener un mayor conocimiento a cerca de la tecnología cisco y comportamiento de las redes. El desarrollo de los escenarios tiene como finalidad llevar a la practica la administración de redes ipv4, ipv6 teniendo en cuenta los protocolos de enrutamiento y las políticas básicas de seguridad de la información.

Palabras clave:

Direccionamiento ip, ipv4, ipv6, ospf, LAN, SSH, router, swicht, VLAN.

ABSTRACT

In the development of this project, the topics of administration, configuration and design of scalable networks will be addressed. this is how the CCNA CISCO deepening diploma (LAN / WAN), allows you to have a greater knowledge about cisco technology and network behavior. The development of the scenarios aims to implement the administration of ipv4, ipv6 networks taking into account routing protocols and basic information security policies.

Keywords:

Addressing ip, ipv4, ipv6, ospf, LAN, SSH, router, swicht, VLAN.

INTRODUCCIÓN

En el presente trabajo tiene como finalidad aplicar los conocimientos adquiridos en el diplomado de profundización CISCO (LAN/WAN), donde el estudiante utilizará los programas de simulación con el fin de desarrollar escenarios LAN/WAN, donde se logrará llevar a cabo las diversas configuraciones de dispositivos, mediante la utilización de la herramienta Packet Tracert.

Como es evidente en la actualidad se evidencio que el direccionamiento ipv4 fue agotando sus direcciones, llevando a una revisión detallada del direccionamiento de redes, donde se concluyó que una de las soluciones para evitar el desperdicio de host es el subnetting el cual direcciona las IP necesarias en la red.

Es así como el presente trabajo mediante la modalidad adoptada por el diplomado de profundización “Proyecto Aplicado” permitirá configurar los dispositivos de los escenarios 1 y 2.

Finalmente, el trabajo se verá culminado con la entrega del documento y los archivos de simulación.

DESARROLLO.

1. Escenario 1

Paso 1. Topología escenario 1

Figura 1. Topología escenario 1

Fuente: propia

Paso 2. Simulación de escenario 1en Packet Tracer.

Figura 2. Simulación de escenario 1en Packet Tracer.

Fuente: propia.

Paso 3. Direccionamiento ip

Desarrollo de esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts y asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1. Direccionamiento ip

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
LAN 1	100	192.168.36.0/ 25	192.168.36.1	192.168.36.126	192.168.36.127
LAN 2	50	192.168.36.128/26	192.168.36.129	192.168.36.190	192.168.36.191

Dispositivo	Interfaz	Dirección	Máscara de subred	Gateway predeterminado
R-1	G0/0/1	192.168.36.1	255.255.255.128	No aplica
	G0/0/0	192.168.36.129	255.255.255.192	No aplica
S SVI	VLAN 1	192.168.36.2	255.255.255.128	192.168.36.1
PC-A	NIC	192.168.36.126	255.255.255.128	192.168.36.1
PC B	NIC	192.168.36.190	255.255.255.192	192.168.36.129

Fuente: propia

Paso 4. Configuración básica del R1.

Tabla 2. Documentación de configuración R1

Configuración	Documentación
Router>enable	Permite el ingreso de configuración global.
Router#configure terminal	Permite la configuración del terminal
Enter configuration commands, one per line. End with CNTL/Z.	Information para ingresar commandos
Router(config)#no ip domain-lookup	comando para desactivar la búsqueda DNS
Router(config)#hostname R1	Permite la configuración del nombre Router
R1(config)#ip domain-name ccna-lab.com	Configuración del nombre del domino
R1(config)#enable secret ciscoenpass	Comando para contraseña cifrada para el modo EXEC privilegiado
R1(config)#line console 0	Ingresamos a la línea de consola
R1(config-line)#password ciscoconpass	Permite asignar la contraseña de acceso a la consola
R1(config-line)#login	Activamos el acceso mediante Loguin
R1(config-line)#exit	
R1(config)#security passwords min-length 10	Comando para establecer la longitud mínima para las contraseñas
R1(config)#username admin password admin1pass	El comando permite crear un usuario administrativo en la base de datos local
R1(config)#line vty 0 4	Instrucción para configurar el inicio de sesión en las líneas VTY para que use la base de datos local
R1(config-line)#password ciscocisco	Comando para asignar contraseña
R1(config-line)#login local	Activamos el acceso para que use la base de datos local
R1(config-line)#transport input SSH	Instrucción que permite configurar VTY solo aceptando SSH
R1(config-line)#exit	Salimos de la configuración de la línea vty
R1(config)#service password-encryption	Comando para cifrar las contraseñas de texto no cifrado
R1(config)#banner motd # Este es el router de la empresa de REDJF, cualquier ingreso no autorizado tendra consecuencias legales #	Instrucción para configurar un MOTD Banner informativo.
R1(config)#interface g0/0/0	Ingreso a la configuración de la interfaz G0/0/0
R1(config-if)#description esta es la interfaz de la LAN 2	Comando para crear descripción de la red.

R1(config-if)#ip address 192.168.36.129 255.255.255.192	Permite la asignación de la dirección Ip y su respectiva mascara.
R1(config-if)#no shutdown	Comando para subir o activar la configuración
R1(config-if)#	
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up	Mensaje de carga de la interfaz.
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up	La interface ha sido activada
R1(config-if)#exit	Regresamos a la configuración del terminal
R1(config)#interface g0/0/1	Comando para ingresas a la interfaz g0/0/1
R1(config-if)#description esta es la interfaz de la LAN 1	Configuración de la interfaz
R1(config-if)#ip address 192.168.36.1 255.255.255.128	Comando para asignar direccion Ip y su mascara de red
R1(config-if)#no shutdown	Comando para subir o activar la configuración
R1(config-if)#	
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up	Mensaje de carga de la interfaz.
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up	Informa que la interfaz ha sido activada
R1(config-if)#exit	Salimos de la configuración de g0/0/1
R1(config)#ip domain-name ccna-lab.com	Comando para llamar al dominio de la red
R1(config)#crypto key generate rsa	Instrucción para encriptar una clave de cifrado RSA
The name for the keys will be: R1.ccna-lab.com	Observamos la respuesta de la instrucción
Choose the size of the key modulus in the range of 360 to 2048 for your	Observamos el tamaño del rango
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.	Información sobre las llaves de uso
How many bits in the modulus [512]: 1024	Finalmente generar una clave de cifrado RSA de 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	Finalmente obtenemos la aceptación de la configuración.

Fuente: propia

Paso 6. Configuración básica del S1

Tabla 3. Documentación de configuración S1

Configuración	Documentación
Switch>enable	Comando para ingresas a la configuración global
Switch#configure terminal	Comando de configuración del terminal
Enter configuration commands, one per line. End with CNTL/Z.	Information para ingresar commandos
Switch(config)#no ip domain-lookup	Permite desactivar la búsqueda DNS
Switch(config)#hostname S1	instrucción para la configuración del nombre Router
S1(config)#ip domain-name ccna-lab.com	Configuración del nombre del domino
S1(config)#enable secret ciscoenpass	Comando para contraseña cifrada para el modo EXEC privilegiado
S1(config)#line console 0	Permite ingresar a la línea de consola
S1(config-line)#password ciscoconpass	Permite asignar la contraseña de acceso a la consola
S1(config-line)#login	Activa el ingreso de mediante login
S1(config-line)#exit	Regresamos a la configuración del terminal
S1(config)#username admin password admin1pass	El comando permite crear un usuario administrativo en la base de datos local
S1(config)#line vty 0 15	comando para configurar el inicio de sesión en las líneas VTY para que use la base de datos local
S1(config-line)#password ciscocisco	Asignación de contraseña
S1(config-line)#login local	Activamos el acceso para que use la base de datos local
S1(config-line)#transport input SSH	Permite configurar VTY solo aceptando SSH
S1(config-line)#exit	Salimos de la configuración línea vty
S1(config)#service password-encryption	Instrucción para encriptar las contraseñas de texto no cifrado
S1(config)#banner motd # Este es el switch1 de la empresa de REDJF, cualquier ingreso no autorizado tendra consecuencias legales #	La instrucción permite configurar el mensaje de banner informativo y de alerta.
S1(config)#ip domain-name ccna-lab.com	Instrucción para llamar al dominio de la red
S1(config)#crypto key generate rsa	comando para encriptar una clave de cifrado RSA
The name for the keys will be: S1.ccna-lab.com	Observamos la respuesta de la instrucción

Choose the size of the key modulus in the range of 360 to 2048 for your	Observamos el tamaño del rango
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.	Información sobre las llaves de uso
How many bits in the modulus [512]: 1024	Configurarnos para generar una clave de cifrado RSA de 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	Obtenemos la aceptación de la configuración.
S1(config)#interface vlan 1	Configurar la interfaz de administración (SVI)
*Mar 1 2:9:56.484: %SSH-5-ENABLED: SSH 1.99 has been enabled	Obtenemos la hora de ingreso a esta configuración.
S1(config-if)#ip address 192.168.36.2 255.255.255.128	Configuramos la dirección Ip y su mascara para Vlan 1
S1(config-if)#no shutdown	Comando para activar la interfaz
S1(config-if)#	
%LINK-5-CHANGED: Interface Vlan1, changed state to up	Obesrvamos como respuesta que la interfaz a sido cargada.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up	Vlan ha sido activada
S1(config-if)#exit	Regresamos a configuración del terminal.
S1(config)#ip default-gateway 192.168.36.1	Finalmente configuramos la dirección del gateway predeterminado

Fuente: propia

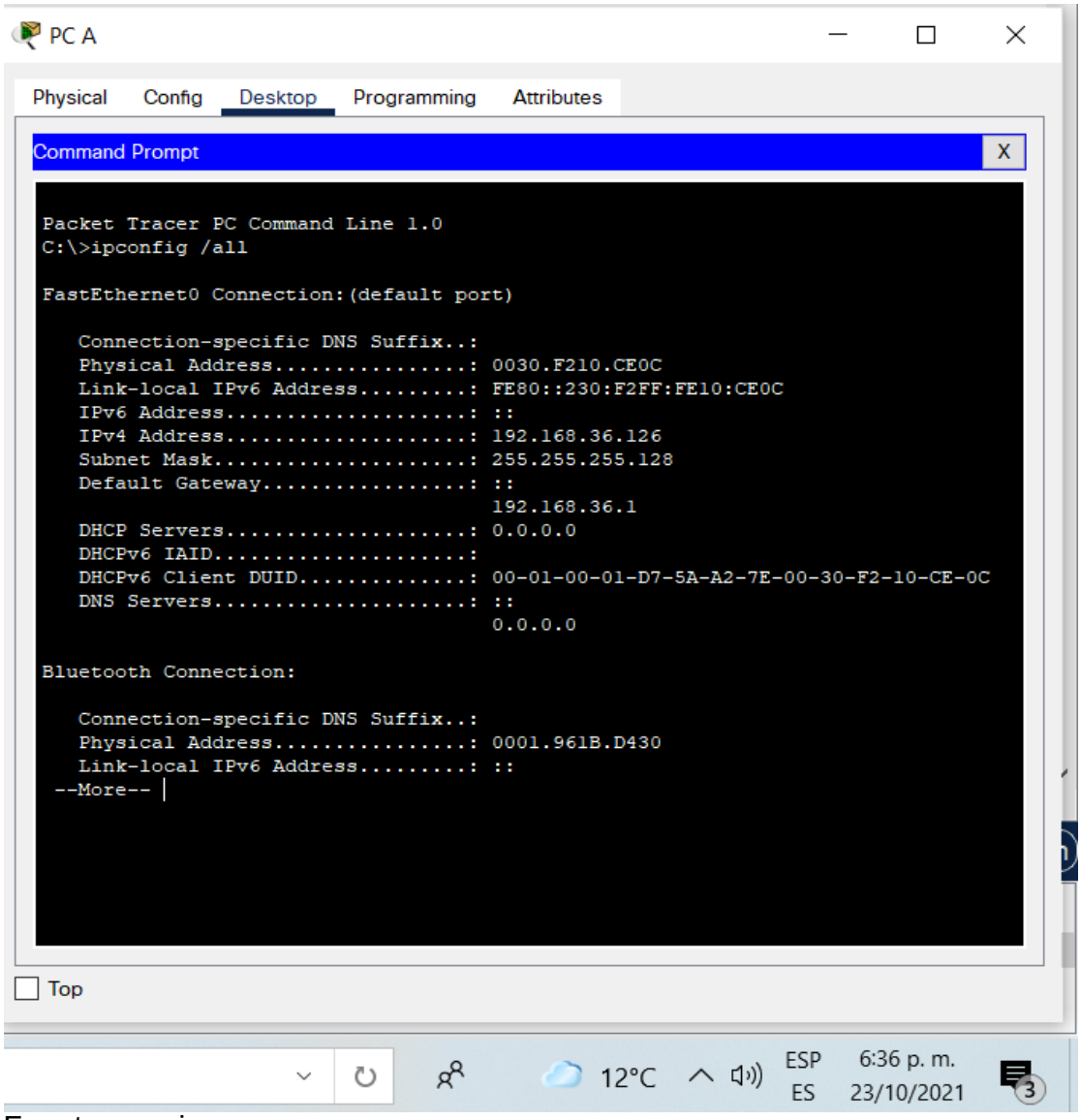
Paso 8. Información de configuración del PC-A

Tabla 4. Información de configuración del PC-A

PC-A Network Configuration	
Descripción	Este es el equipo PC-A
Dirección física	030.F210.CE0C
Dirección IP	192.168.36.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.36.1

Fuente: propia

Figura 3. Configuración física del PC-A



Fuente: propia

C:\>ipconfig /all
.

Permite obtener la configuración del pc con cada una de sus direcciones.

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address. 0030.F210.CE0C
Link-local IPv6 Address. ..... : FE80::230:F2FF:FE10:CE0C
IPv6 Address. ..... : ::
IPv4 Address. ..... : 192.168.36.126
Subnet Mask. ..... : 255.255.255.128

Default Gateway. ..... : ::
192.168.36.1
DHCP Servers. ..... : 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-D7-5A-A2-7E-00-30-F2-10-CE-0C
DNS Servers. .....: ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address.....: 0001.961B.D430
Link-local IPv6 Address..... : ::

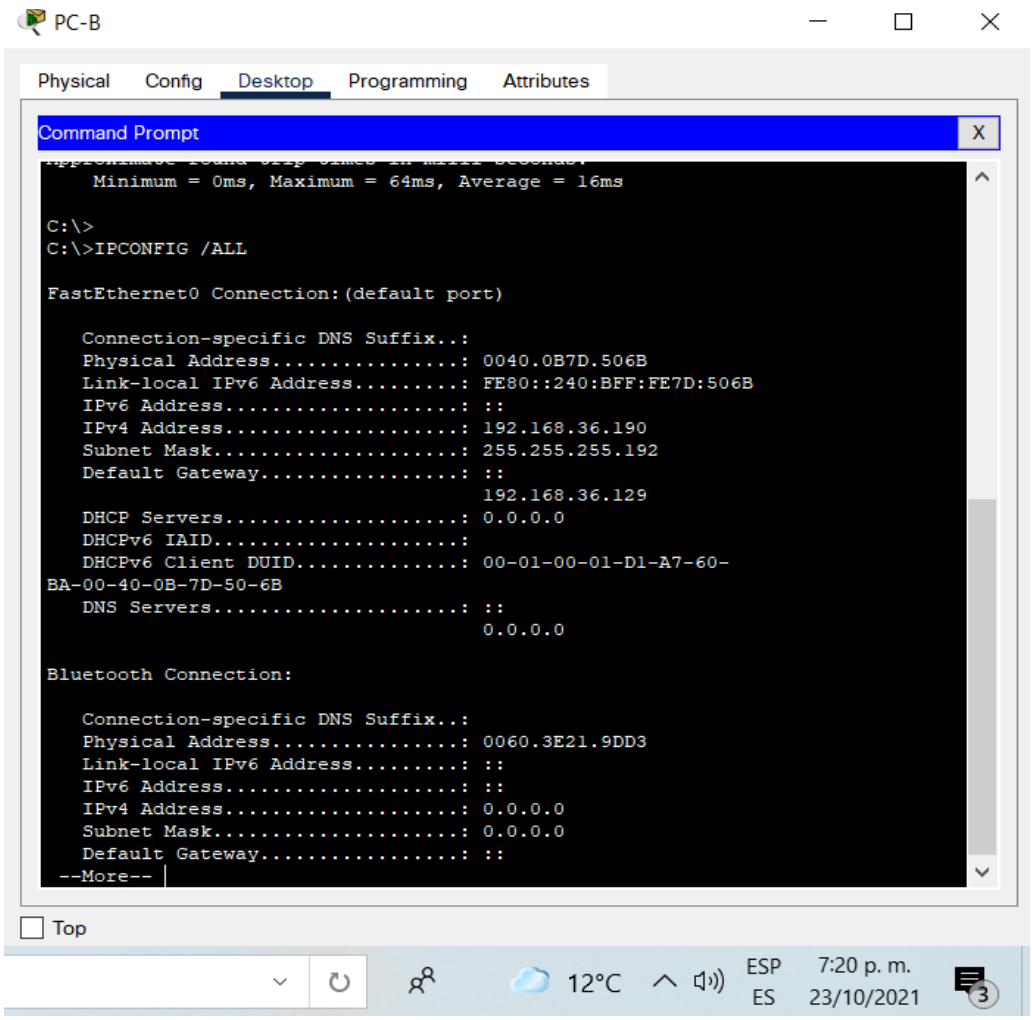
Paso 9. Información de configuración del PC-B

Tabla 5. Información de configuración del PC-B

PC-B Network Configuration	
Descripción	Este es el PC- B
Dirección física	0040.0B7D.506B
Dirección IP	192.168.36.190
Máscara de subred	255.255.255.192
PC-B Network Configuration	
Gateway predeterminado	192.168.36.129

Fuente: propia

Figura 4. Configuración básica del PC-B



Fuente: propia

C:\>ipconfig /all
.

Permite obtener la configuración del pc con cada una de sus direcciones.

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:
Physical Address. 0040.0B7D.506B
Link-local IPv6 Address. ..... : FE80::240:BFF:FE7D:506B
IPv6 Address. ..... : ::
IPv4 Address. ..... : 192.168.36.190
Subnet Mask. ..... : 255.255.255.192
Default Gateway. ..... : ::
192.168.36.129
DHCP Servers. ..... : 0.0.0.0
DHCPv6 IAID.....:

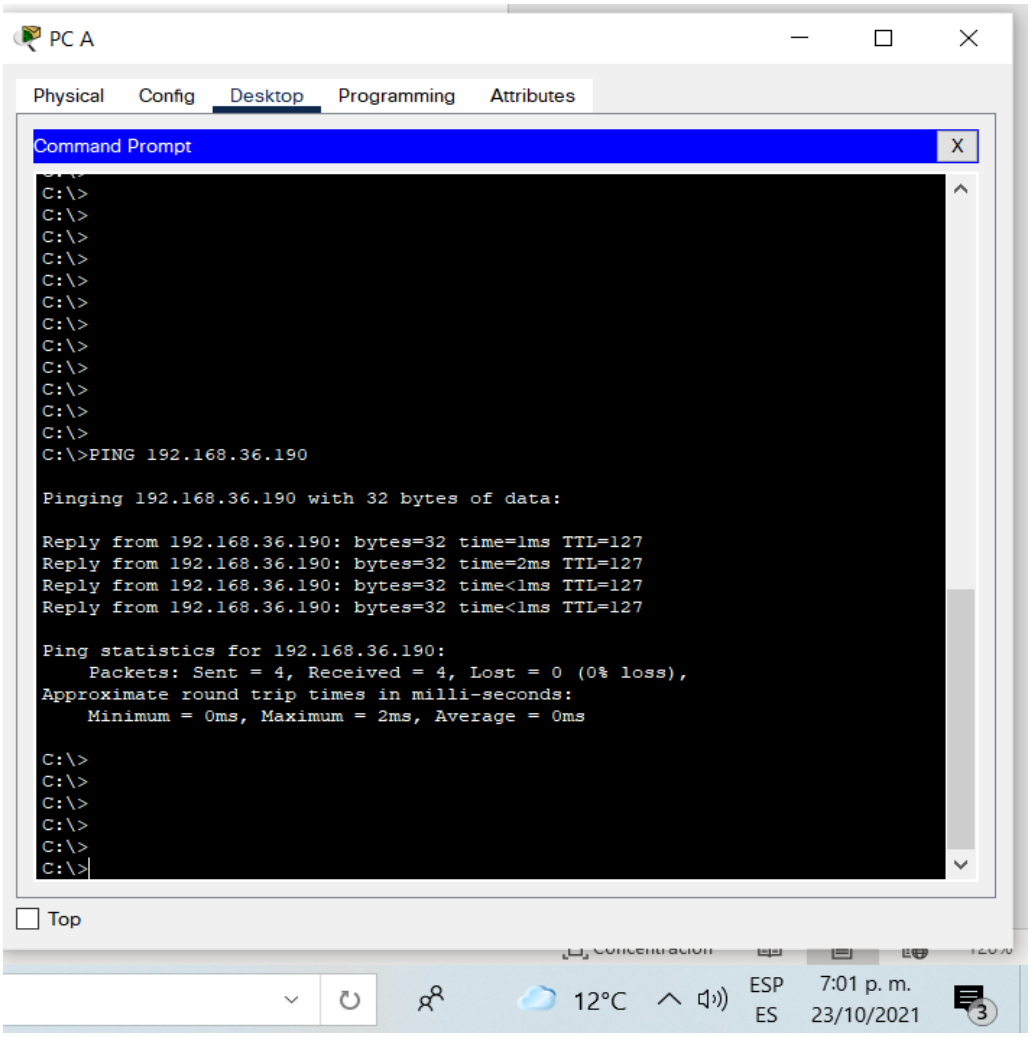
DHCPv6 Client DUID..... 00-01-00-01-D1-A7-60-BA-00-40-0B-7D-50-6B
DNS Servers. ..... : ::
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix..:
Physical Address.....: 0060.3E21.9DD3
Link-local IPv6 Address..... : ::

Paso 10. Evidencias de pruebas de ping desde al PC-A a PC-B y viseversa.

Figura 5. Evidencia de ping desde al PC-A a PC-B



Fuente: propia.

Prueba de conexión mediante el comando ping desde la PC-A a PC-B,

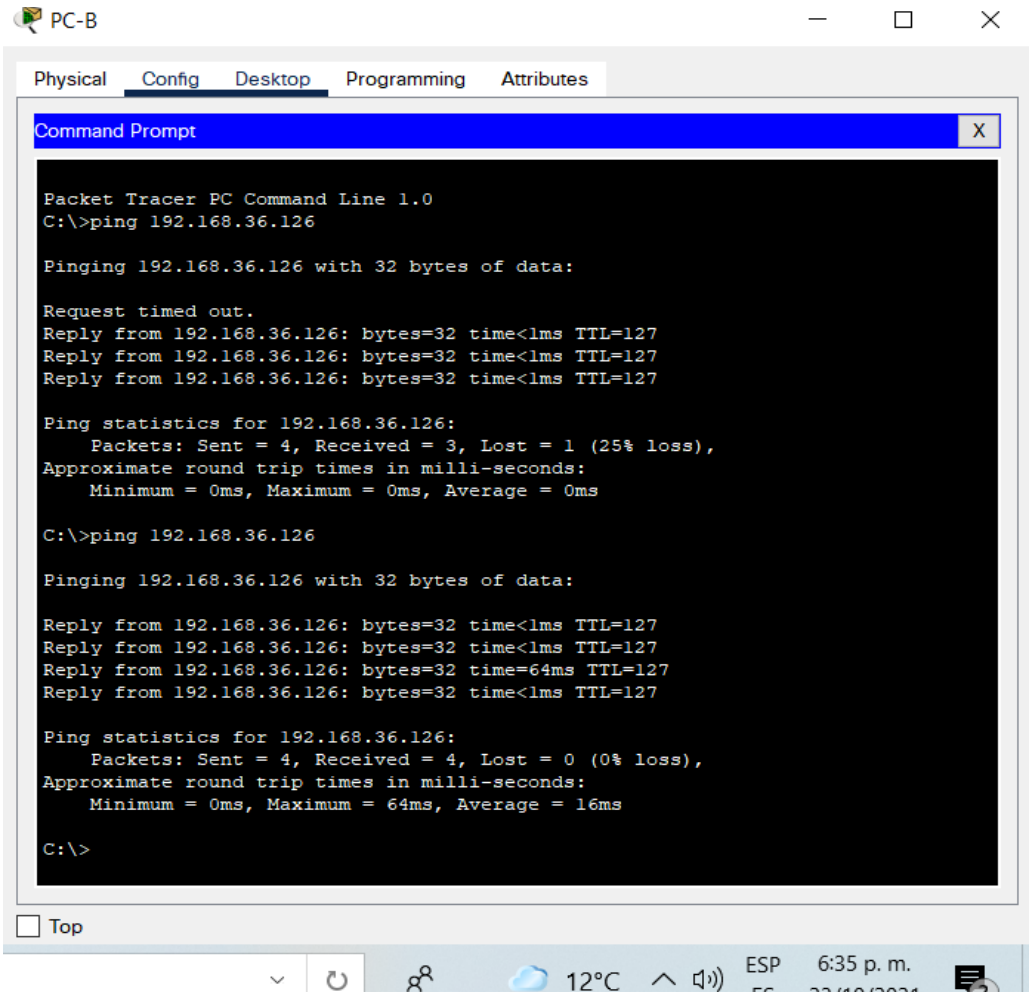
PING 192.168.36.190 permite comprobar la conectividad entre equipos

Pinging 192.168.36.190 with 32 bytes of data:

Reply from 192.168.36.190: bytes=32 time=1ms TTL=127
Reply from 192.168.36.190: bytes=32 time=2ms TTL=127
Reply from 192.168.36.190: bytes=32 time<1ms TTL=127
Reply from 192.168.36.190: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.36.190:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms

Figura 6. Evidencia de ping desde al PC-B a PC-A



Fuente: propia.

Prueba de conexión mediante el comando ping desde la PC-B a PC-A, adjunto código de conexión.

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.36.126 Comando para comprobar conexión

Pinging 192.168.36.126 with 32 bytes of data:

Request timed out.
Reply from 192.168.36.126: bytes=32 time<1ms TTL=127
Reply from 192.168.36.126: bytes=32 time<1ms TTL=127
Reply from 192.168.36.126: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.36.126:
Packets: Sent = 4, Received = 3, Lost = 1(25% loss),evidencia que se pierde 25 %
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.36.126

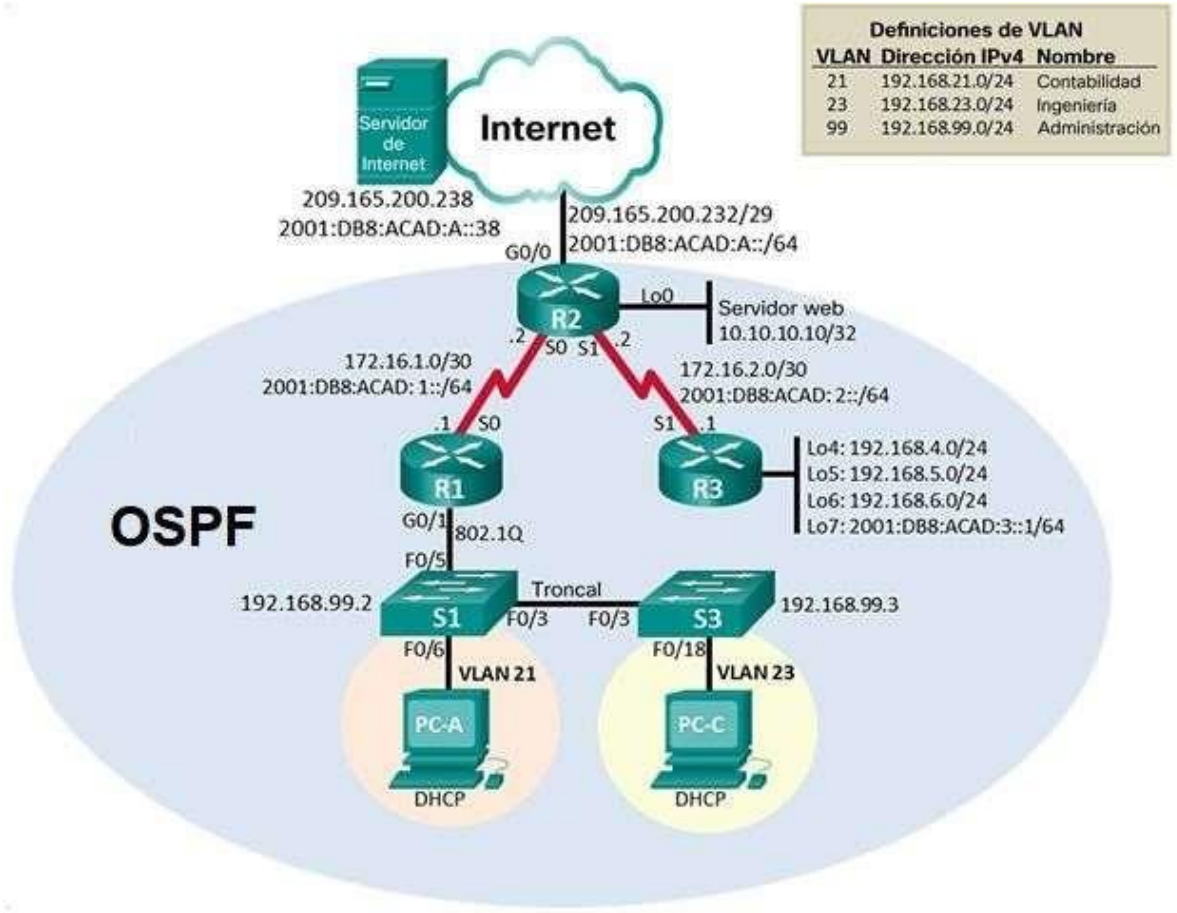
Pinging 192.168.36.126 with 32 bytes of data:

Reply from 192.168.36.126: bytes=32 time<1ms TTL=127
Reply from 192.168.36.126: bytes=32 time<1ms TTL=127
Reply from 192.168.36.126: bytes=32 time=64ms TTL=127
Reply from 192.168.36.126: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.36.126:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), no se pierden paquetes.
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 64ms, Average = 16ms

2. Escenario 2

Figura 7. Topología escenario 2

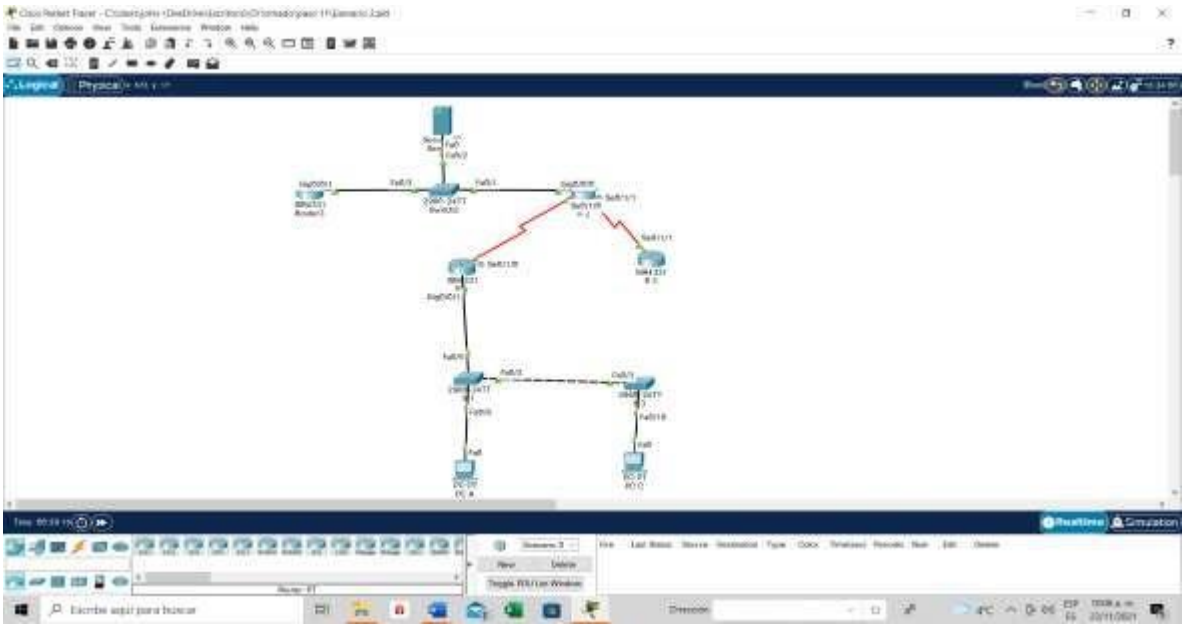


Fuente: Topología requerida por la práctica de habilidades CCNA escenario 2.

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.

Paso 1. Simulación de escenario 2 en Packet Tracer.

Figura 8. escenario 2 en Packet Tracer



Fuente: propia

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 6. Comandos para Inicializar a cargar los dispositivos.

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

Fuente: propia

Parte 2:Configurar los parámetros básicos de los dispositivos

Paso 2: Configurar la computadora de Internet

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

Tabla 7. Configuración de parámetros básicos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/64
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración de R1

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 s R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#pas R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#pass 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 red JF#

Interfaz S0/0/0	R1(config)#int s0/1/0 R1(config-if)#description interface hacia el router R2 R1(config-if)#exit R1(config)#ipv6 uni R1(config)#ipv6 unicast-routing R1(config)#int s0/1/0 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 sh R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 S0/1/0 R1(config)#

Fuente: propia

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuracion R2

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 s R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#pass 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 server

	^ % Invalid input detected at '^' marker.
Mensaje MOTD	R2(config)#banner motd #se prohibe el acceso no autorizado red JF#
Interfaz S0/1/0	R2(config-if)#description interface desde R1 A R2 R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#int s0/1/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
Interfaz S0/1/1	R2(config)#int S0/1/1 R2(config-if)#description conexion de R2 a R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0/0 R2(config-if)#description interface hacia internet R2(config-if)#exit R2(config)#in R2(config)#ipv6 u R2(config)#ipv6 unicast-routing R2(config)#int g0/0/0 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 sh
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#description servidor WEB

	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 g0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0/0

Fuente: propia

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

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 console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#pass 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 red JF#
Interfaz S0/1/1	R3(config-if)#description interface desde R3 a R2 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#int s0/1/1 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no sh
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#

	%LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config-if)#ip add 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config-if)#ip add 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#int loopback 6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#ip add 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit.

Fuente: propia

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1

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 s S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#pas S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#pass 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: propia

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración del S3

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 console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login

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: propia

Paso 8: Verificar la conectividad de la red

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

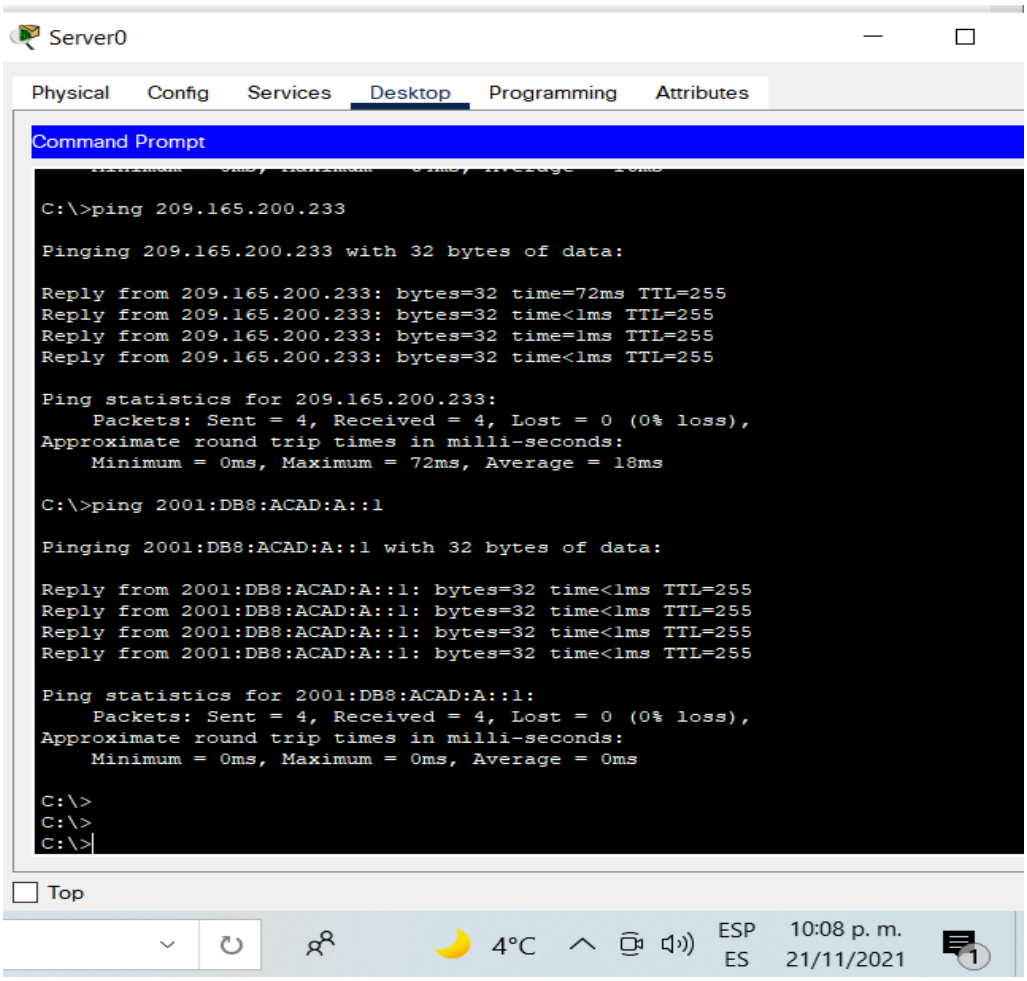
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms
R2	R3, S0/1/1	172.16.2.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/16 ms
PC de Internet	Gateway predeterminado	209.165.200.233	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 = 95ms, Average = 23ms
		2001:DB8:ACAD:A::1	IPV6 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 64ms, Average = 16ms

Figura 9. conectividad de la red por medio del comando ping.



Fuente: propia

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

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración de la seguridad, vlan en el switch s1.

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)#
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up S1(config-if)#ip address 192.16.99.2 255.255.255.0 S1(config-if)#no sh S1(config-if)#no shutdown 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)#int f0/3 S1(config-if)#sw mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S1(config-if)#sw trunk native vlan 1 S1(config-if)#exit

Forzar el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#sw 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)#int range f0/1-f0/2 S1(config-if-range)#sw mode acc S1(config-if-range)#sw mode access S1(config-if-range)#int range f0/7-f0/24 S1(config-if-range)#sw mode access S1(config-if-range)#
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#sw access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/7-f0/24 S1(config-if-range)#sh

Fuente: propia

Paso 10: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración seguridad, vlan en el S3

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)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no sh 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)#int f0/3 S3(config-if)#sw mode trunk S3(config-if)#sw trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	S3(config)#int range f0/1-f0/2 S3(config-if-range)#sw mode access S3(config-if-range)#int range f0/7-f0/24 S3(config-if-range)#sw mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#sw acc vlan 21
Apagar todos los puertos sin usar	S3(config-if)#int range f0/7-f0/17 S3(config-if-range)#sh

Fuente: propia

Paso 11: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/0/1.21 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to up R1(config-subif)#descri R1(config-subif)#description LAN contabilidad R1(config-subif)#enc dot1q 21 R1(config-subif)#ip add 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)#int g0/0/1.23 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up R1(config-subif)#description LAN ingenieria R1(config-subif)#enc 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)#int g0/0/1.99 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up R1(config-subif)#description LAN administracion R1(config-subif)#enc 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)#int g0/0/1 R1(config-if)#no sh

Fuente: propia

Paso 12: Verificar la conectividad de la red

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

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

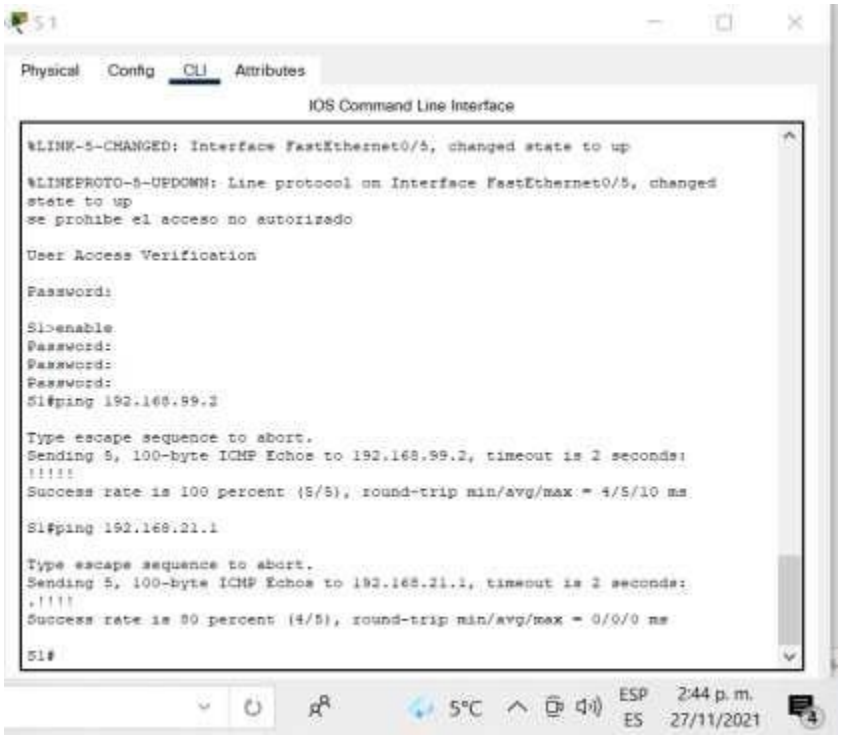
Tabla 17. conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	S1#ping 192.168.99.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:

			!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/6 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, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	92.168.21.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	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 = 0/0/0 ms

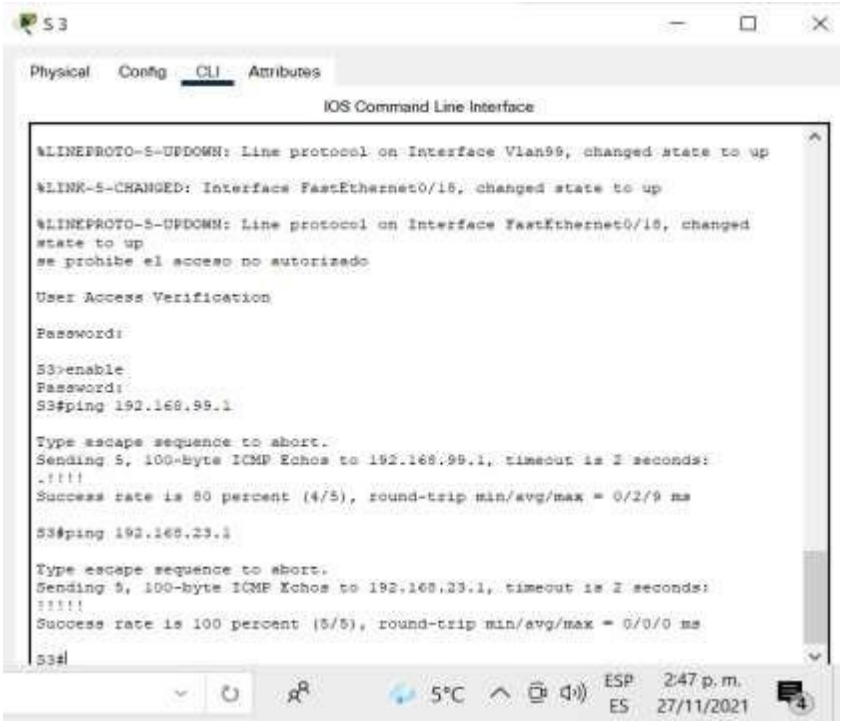
Fuente: propia

Figura 10. Pruebas de conectividad entre el S1 y el R1.



Fuente: propia.

Figura 11. Pruebas de conectividad entre el S3 y el R1.



Fuente: propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 13: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 36
Anunciar las redes conectadas directamente	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 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/0/1 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
Desactive la sumarización automática	No se puede desactivar sumarizacion automática en ospf.

Fuente: propia

Paso 14: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 36
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0

	R2(config-router)# 01:34:05: %OSPF-5-ADJCHG: Process 36, Nbr 192.168.99.1 on Serial0/1/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	No se puede desactivar sumarizacion automática en ospf.

Fuente: propia

Paso 15: Configurar OSPFv6 en el R3.

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración OSPFv6 en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#ipv6 router ospf 37
Anunciar redes IPv4 conectadas directamente	R3(config-rtr)#router-id 2.2.2.2 R3(config-rtr)#exit R3(config)#int s0/1/1 R3(config-if)#ipv6 ospf 37 area 0 R3(config-if)#exit R3(config)#
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config)#int loopback 7 R3(config-if)#ipv6 ospf 37 area 0 R3(config-if)#exit R3(config)#ipv6 router ospf 37 R3(config-rtr)#passive R3(config-rtr)#paassi R3(config-rtr)#passive R3(config-rtr)#passive-interface lo 4 R3(config-rtr)#passive-interface lo 5 R3(config-rtr)#passive-interface lo 6 R3(config-rtr)#
Desactive la sumarización automática.	No se puede en versión ospf.

Fuente: propia

Paso 16: Verificar la información de OSPF

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

Tabla 21.comandos para verificar la información de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#Show ip route
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#Show run

Fuente: propia

Figura 12. información de OSPF comando show.

Fuente: propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración el R1 como servidor de DHCP

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 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#domai R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#dns- R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#defa R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#exit R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 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)#
Crear 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)#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)#

Fuente: propia

Paso 18: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#http server ^ % Invalid input detected at '^' marker.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local ^ % Invalid input detected at '^' marker.
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0/0 R2(config-if)#ip nat out R2(config-if)#ip nat outside R2(config-if)#int s0/1/0 R2(config-if)#ip nat in R2(config-if)#ip nat inside R2(config-if)#int s0/1/1 R2(config-if)#ip nat inside R2(config-if)#int lo R2(config-if)#int lo 0 R2(config-if)#ip nat inside R2(config-if)#
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 192.168.0.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

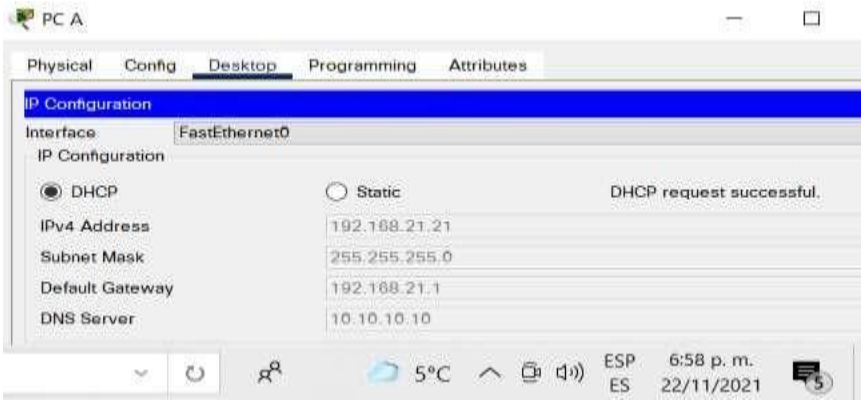
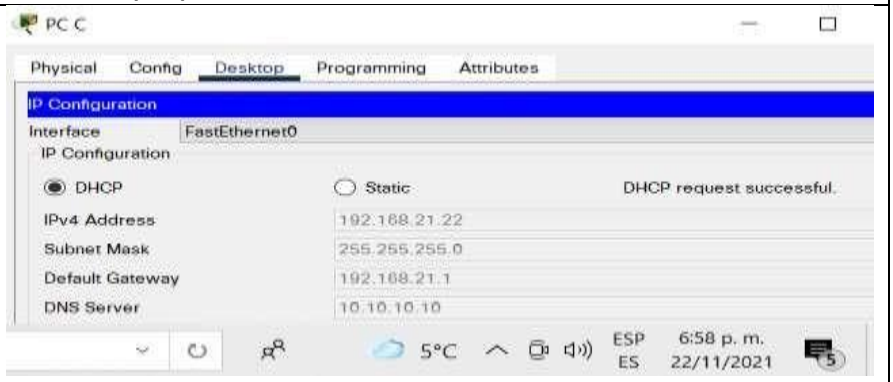
Fuente: propia

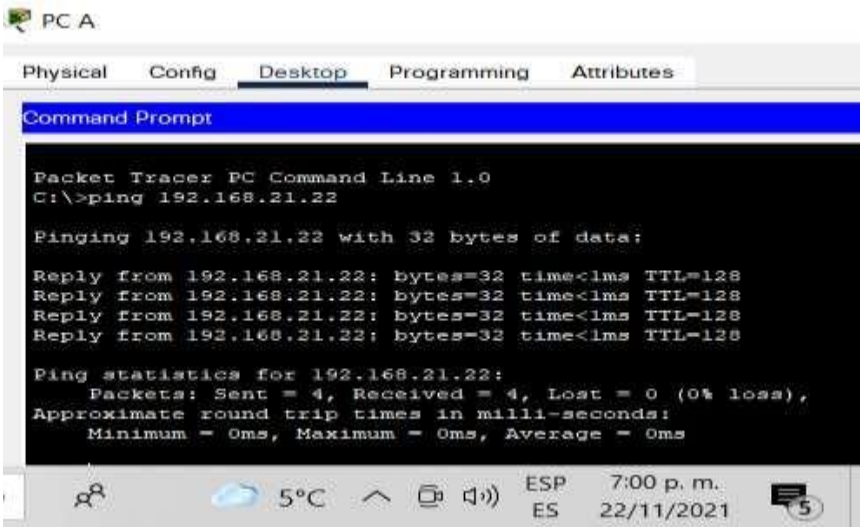
Paso 19: Verificar el protocolo DHCP y la NAT estática

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

Tabla 24. Comandos para verificar el protocolo DHCP y la NAT estática

Figura 13. Evidencias de configuraciones de DHCP y NAT estática

Prueba	Resultados
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	 Fuente: propia

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	 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**	 Fuente: propia

Fuente: propia

Parte 6: Configurar NTP

Tabla 25. Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 march 2016 R2#sh clock 9:0:2.942 UTC Sat Mar 5 2016
Configure R2 como un maestro NTP.	R2(config)# R2(config)#ntp mas

	R2(config)#ntp master 5 R2(config)#exit R2# %SYS-5-CONFIG_I: Configured from console by console sh clock 9:8:19.289 UTC Sat Mar 5 2016
Configurar R1 como un cliente NTP.	R1(config)#ntp ser R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp upda R1(config)#ntp update-calendar R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console
Verifique la configuración de NTP en R1.	R1#sh clock *5:49:38.876 UTC Mon Mar 1 1993 R1#sh clock

Fuente: propia

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

Paso 20: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Configuración de (ACL)

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 access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#deny an R2(config-std-nacl)#deny any

	R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#ip acc R2(config-line)#ip access-class a R2(config-line)#ip access-class ADMIN-MGT in R2(config-line)#trans R2(config-line)#transport in R2(config-line)#transport input te R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Opense prohibe el acceso no autorizado red JF User Access Verification Password: R2>exit [Connection to 172.16.1.2 closed by foreign host]

Fuente: propia

Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. Comandos de CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (2 match(es)) 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.0.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 20 deny any
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters ^ % Invalid input detected at '^' marker.
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface GigabitEthernet0/0/0 is up, line protocol is up (connected) Internet address is 209.165.200.233/29 Broadcast address is 255.255.255.255

	Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is disabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled Router Discovery is disabled
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.233 10.10.10.10 --- --- tcp 209.165.200.225:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translations

Fuente: propia

CONCLUSIONES

- La evolución tecnológica de las redes ha llevado a que el mundo entero se vea inmerso en el mundo del internet, el cual ha tenido que evolucionar para brindar mayor seguridad y conectividad a los usuarios.

- El desarrollo de los escenarios 1 y 2 permito al estudiante recopilar los conocimientos adquiridos en el diplomado CCNA, de este modo la prueba de habilidades CCNA permitió configurar los de manera exitosa y eficiente cada uno de los dispositivos de las redes.

- El desarrollo de los escenarios permitió que el estudiante adquiera los conocimientos básicos para diseñar esquemas de direccionamientos debidamente administrados que evitan el desperdicio de direcciones host dentro de una red, de este modo el desarrollo de los escenarios permitió crear una topología según el direccionamiento y los protocolos de enrutamiento

- En el desarrollo de la actividad se logró configurar los equipos de manera manual y lógica llevando al estudiante a optimizar el funcionamiento de la red.

- Finalmente, la actividad permitió documentar de manera detallada las diferentes pruebas de conectividad en los equipos de la red mediante los comandos ping, traceroute y show ip route.

BIBLIOGRÁFIA

[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]Sandoval, K. J. (1989). Prueba de habilidades CCNA 2019.. [Curso de Profundización, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/27323.

[9]Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

[10]Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

[11] CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

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

[14] CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

[15] 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.