

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

HAROL ALEXANDER VARGAS BAQUERO

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

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

HAROL ALEXANDER VARGAS

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

DIRECTOR:
ING. RAUL BAREÑO

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 28 de noviembre de 2021

AGRADECIMIENTOS

Un especial agradecimiento a mi familia, quien me apoyado incondicionalmente en cada etapa de mi formación y en las decisiones tomadas.

Gracias a mis padres por ser los principales pilares que soportaron e incentivaron mis sueños, mis anhelos de formarme profesional y personalmente. Gracias a mi mamá por estar siempre presente brindándome su cariño y acompañamiento incondicional, por su incomparable capacidad para motivarme en los momentos más difíciles y adversos. Gracias a mi Padre por inculcarme los valores y ética que hoy definen quien soy y la forma en que afronto las situaciones cotidianas y académicas, espero desde donde se encuentre puede seguir guiándome en el camino de la integridad, el amor y la ética. Gracias a mi hermano quien con su sed insaciable de conocimiento representa un modelo a seguir para continuar y superarme constantemente. Gracias a las demás personas y conocidos que siempre se encuentran ahí motivándome para seguir adelante.

Gracias a la universidad Nacional abierta y a distancia (UNAD), ya que por su metodología de educación me permitió cursar el programa de formación y cumplir el sueño de capacitarme para la vida personal y laboral.

Finalmente, infinitas gracias a Dios por brindarme una familia amorosa y unida, por mis padres, por la salud para cada persona cerca de mi vida, la cual permitió el desarrollo de este diplomado de profundización.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN	10
DESARROLLO	11
CONCLUSIONES	39
BIBLIOGRAFÍA.....	40

LISTA DE TABLAS

Tabla 1 tabla de direccionamiento	12
Tabla 2 Asignación de direcciones IP	12
Tabla 3 Información PC-A.....	15
Tabla 4 Información PC-B.....	16
Tabla 5 Eliminación de configuración de inicio	18
Tabla 6 Parámetros de configuración	19
Tabla 7 Pruebas de conectividad.....	24
Tabla 8 Prueba de conectividad.....	28
Tabla 9 Pruebas protocolo DHCP y NAT estática.....	33
Tabla 10 Lista de comandos	36

LISTA DE FIGURAS

Figura 1 Topología escenario 1	11
Figura 2 Topología de red en packet tracer	11
Figura 3 ipconfig/all PC-A	15
Figura 4 ipconfig/all PC-B	16
Figura 5 Topología escenario 2	17
Figura 6 Topología 2 en packet tracer	18
Figura 7 Ping de R2 a S0/2/0 de R3	25
Figura 8 Ping de R1 a S0/2/0 de R2	25
Figura 9 Ping de PC de internet a Gateway predeterminado.....	25
Figura 10 Ping de S3 a Vlan 23	29
Figura 11 Pin de S1 a Vlan 99	29
Figura 12 Ping de S3 a Vlan 99	29
Figura 13 Ping de S1 a Vlan 21	29
Figura 14 Comandos OSPF.....	31
Figura 15 Comando Show ip protocols	31
Figura 16 Comando Show ip route ospf.....	32
Figura 17 Comando Show running	32
Figura 18 Dirección IP tomada por DHCP en PC-A	34
Figura 19 Dirección IP tomada por DHCP en PC-C.....	34
Figura 20 PING de PC-A a PC-C.....	35
Figura 21 Conexión al servidor web desde PC-A	35
Figura 22 Comando Show access-list.....	36
Figura 23 Comando show ip interface	37
Figura 24 Comando Show ip nat translations	37
Figura 25 Comando Clear ip nat translation	37

GLOSARIO

Interfaz: Se refiere al componente de hardware que permite que un dispositivo pueda conectarse a una red cualquiera.

Subnetting: Corresponde a una técnica utilizada en telecomunicaciones para dividir redes en distintas subredes o redes más pequeñas.

Topología de red: Se puede definir como un mapa físico o lógico de una red para intercambiar datos, contiene la disposición de la red, incluyendo sus nodos, dispositivos y líneas de conexión.

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.

Comando: es una instrucción que el usuario proporciona a un sistema informático, desde la línea de órdenes (como una Shell) o desde una llamada de programación. Puede ser interno (contenido en el propio intérprete) o externo (contenido en un archivo ejecutable).

RESUMEN

El desarrollo de este documento presenta la solución de los escenarios que buscan probar las habilidades de los estudiantes del diplomado de profundización de cisco, en el cual se comprueban los conocimientos obtenidos de redes y dispositivos de red.

Para dar solución a los escenarios propuestos, se planteó el desarrollo de actividades de lectura y pruebas técnicas que le permiten a los estudiantes desarrollar las habilidades necesarias para abordar las actividades planteadas.

Para resolver el escenario número uno, se realizó la topología de red en el software de simulación Cisco Packet Tracer, luego se realizará la distribución de redes y subredes con su respectivo enrutamiento, y, por último, con la ayuda de los comandos adquiridos en el proceso de aprendizaje y mediante un ingreso a los dispositivos de red por la línea de consola, se configurará los requerimientos técnicos de la guía de aprendizaje.

En el escenario numero dos luego de construir la topología de red indicada, se verán a fondo temas del curso de cisco CCNA II incluyendo características que permiten mejorar la seguridad, la eficiencia y la sencillez de la red.

Palabras claves: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

The development of this document presents the solution of the scenarios that seek to test the skills of the students of the cisco deepening diploma course, in which the knowledge obtained on networks and network devices is tested.

To solve the proposed scenarios, we proposed the development of reading activities and technical tests that allow students to develop the necessary skills to address the proposed activities.

To solve scenario number one, the network topology was performed in the simulation software Cisco Packet Tracer, then the distribution of networks and subnets with their respective routing, and finally, with the help of the commands acquired in the learning process and by entering the network devices by console line, the technical requirements of the learning guide will be configured.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics

INTRODUCCIÓN

Las telecomunicaciones hoy en día abarcan una gran gama de herramientas muy importantes para la sociedad en su ámbito laboral y personal, ya que brindan una forma sencilla y fácil de comunicar personas que por diversos motivos (geográficos, económicos, sociales, etc.) antes no lo podían hacer. Es debido a esto que toda persona que se encuentre involucrada en el ámbito de las telecomunicaciones y/o tecnologías debe contar con los conocimientos mínimos requeridos para administrar dispositivos de telecomunicaciones y mantener la red en funcionamiento.

El presente documento corresponde al desarrollo de los escenarios propuestos en el diplomado de profundización cisco (Diseño e implementación de soluciones integradas LAN/WAN), que pretende evaluar los conocimientos adquiridos sobre router, switch, servidores y demás dispositivos de infraestructura de red proporcionados por cisco, adicionalmente, se pondrán a prueba las habilidades de los estudiantes para el diseño, implementación y soporte de redes, principalmente de tipo LAN y WAN, con todos los parámetros que esto conlleva (direccionamiento ip, subnetting, interfaces, puertos, etc.).

Para el desarrollo de las actividades propuestas o "escenarios", se usó como base todos los conceptos y material en la plataforma de cisco dispuesta para el curso, los cuales se sugieren revisar a la par de este trabajo para un mejor entendimiento y conceptualización.

DESARROLLO

1. Escenario 1

Figura 1 Topología escenario 1



Fuente: Autor

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 switch S1, y los PC. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1

Se implementa la topología de red de la figura 1, se cablea según las indicaciones y se agregan cables de consola al switch y router que se utilizaran posteriormente.

Figura 2 Topología de red en packet tracer



Fuente: Autor

Parte 2

Para la parte dos se realiza la siguiente tabla de direccionamiento teniendo en cuenta que el número de documento (c.c.) termina en 13.

Tabla 1 tabla de direccionamiento

Red	host	Mascara de sub red	Dirección IP de la red	Primera IP util	Ultima IP util	broadcast	Host disponible
LAN 1	100	255.255.255.128	192.168.13.0/25	192.168.13.1	192.168.13.126	192.168.13.127	126
LAN 2	50	255.255.255.192	192.168.13.128/26	192.168.13.129	192.168.13.190	192.168.13.191	62

Fuente: Autor

Tabla 2 Asignación de direcciones IP

Item	Requerimiento
Dirección de red	192.168.13.0
Requerimiento de Subred LAN1	100 (Se asignará una red de 126 host disponibles)
Requerimiento de Subred LAN2	50 (Se asignará una red de 62 host disponibles)
R1 G0/0/1	192.168.13.1/25
R1 G0/0/0	192.168.13.129/26
S1 SV1	192.168.13.2/25
PC-A	192.168.13.126/25
PC-B	192.168.13.190/26

Fuente: Autor

Parte 3

A continuación, se describe el código implementado en el router y switch que contiene la configuración establecida en la guía de actividades.

Router R1

Código	Descripción
Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#hostname R1	Asigno nombre al router R1
R1(config)#no ip domain-lookup	Comando para desactivar la búsqueda DNS
R1(config)#ip domain-name ccna-lab.com	Asignación dominio ccna-lab.com
R1(config)#enable secret ciscoenpass	Cifra la contraseña exec privilegiado
R1(config)#line console 0	Asignación de contraseña de acceso a la consola
R1(config-line)#password ciscoenpass	
R1(config-line)#login	

R1(config)#security password min-length 10	Se establece la longitud mínima para las contraseñas a 10 caracteres.
R1(config)#username admin password admin1pass	Creación de usuario administrativo en la base de datos local
R1(config)#line vty 0 4	Se configura el inicio de sesión en las líneas vty con la base de datos local
R1(config-line)#login local	Configurar VTY solo aceptando SSH
R1(config-line)#transport input ssh	Asignación del banner motd de acceso a router 1
R1(config)#banner motd "El acceso a este dispositivo está restringido para instructores y alumnos de la UNAD"	
R1(config)#interface gigabitethernet 0/0/0	Asignación de ip para la interfaz Gigabitethernet 0/0/0
R1(config-if)#ip address 192.168.13.129 255.255.255.192	Se enciende la interfaz
R1(config-if)#no shutdown	
R1(config)#interface gigabitethernet 0/0/1	Asignación de ip para la interfaz Gigabitethernet 0/0/1
R1(config-if)#ip address 192.168.13.1 255.255.255.128	Se enciende la interfaz
R1(config-if)#no shutdown	
R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024	Se genera una clave de cifrado RSA con módulo de 1024

Configuraciones en el switch S1

Las configuraciones realizadas en el switch son las siguientes:

Código	Descripción
Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname S1	Asigno nombre al switch S1
S1(config)#no ip domain-lookup	Comando para desactivar la búsqueda DNS
S1(config)#ip domain-name ccna-lab.com	Asignación dominio ccna-lab.com
S1(config)#enable secret ciscoenpass	Cifra la contraseña exec privilegiado
R1(config)#line console 0	Asignación de contraseña de acceso a la consola
S1(config-line)#password ciscoconpass	
S1(config-line)#login	

S1(config)#username admin password admin1pass	Creación de usuario administrativo en la base de datos local
S1(config)#line vty 0 15	Se configura el inicio de sesión en las líneas vty con la base de datos local
S1(config-line)#login local	Configurar VTY solo aceptando SSH
S1(config-line)#transport input ssh	Asignación del banner motd de acceso a switch 1
S1(config)#banner motd "El acceso de este dispositivo está autorizado únicamente para personal de la UNAD"	
S1(config)#interface vlan 1	Asignación de ip para la interfaz VLAN1
S1(config-if)#ip address 192.168.13.2 255.255.255.128	
S1(config-if)#no shutdown	Se enciende la interfaz
S1(config)#crypto key generate rsa	Se genera una clave de cifrado RSA con módulo de 1024
The name for the keys will be:	
S1.ccna-lab.com	
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.	
How many bits in the modulus [512]:	
1024	
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	

Paso 2

Luego de la configuración del router y el switch, se procede a configurar los hosts y se obtiene la siguiente configuración.

Figura 3 ipconfig/all PC-A

```

Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 00D0.9746.ACBB
    Link-local IPv6 Address.....: FE80::2D0:97FF:FE46:ACBB
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.13.126
    Subnet Mask.....: 255.255.255.128
    Default Gateway.....: ::
                                0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-8E-A0-0A-27-00-D0-97-46-AC-BB
    DNS Servers.....: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 0001.97D8.E19C
    Link-local IPv6 Address.....: ::
--More-- |

```

Fuente: Autor

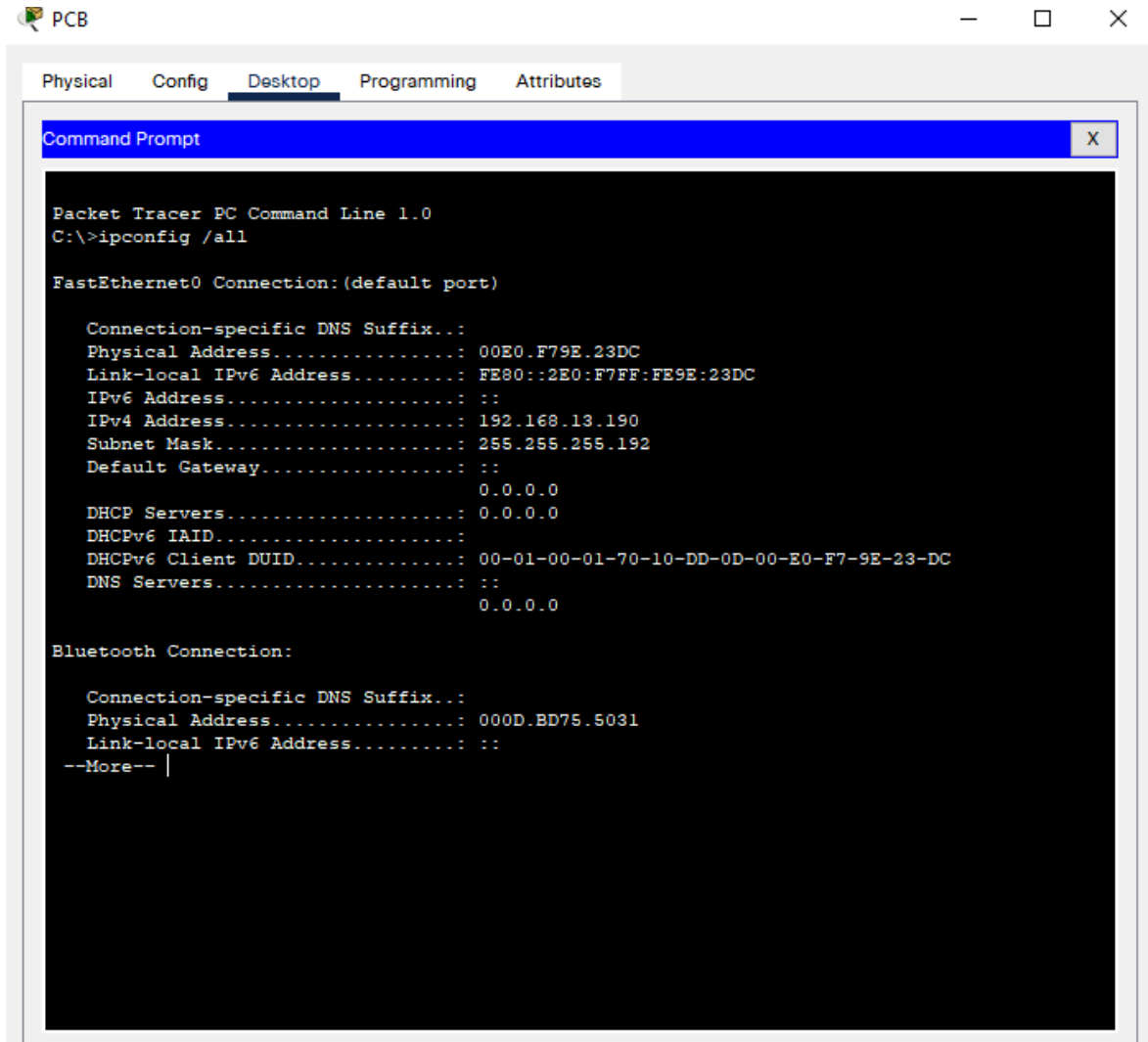
Tabla 3 Información PC-A

PC-A Network Configuration	
Descripción	PC-A para 100 host
Dirección física	00D0.9746.ACBB
Dirección IP	192.168.13.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.13.1

Fuente: Autor

Se realiza el mismo proceso para el PC-B de la siguiente red LAN

Figura 4 ipconfig/all PC-B



Fuente: Autor

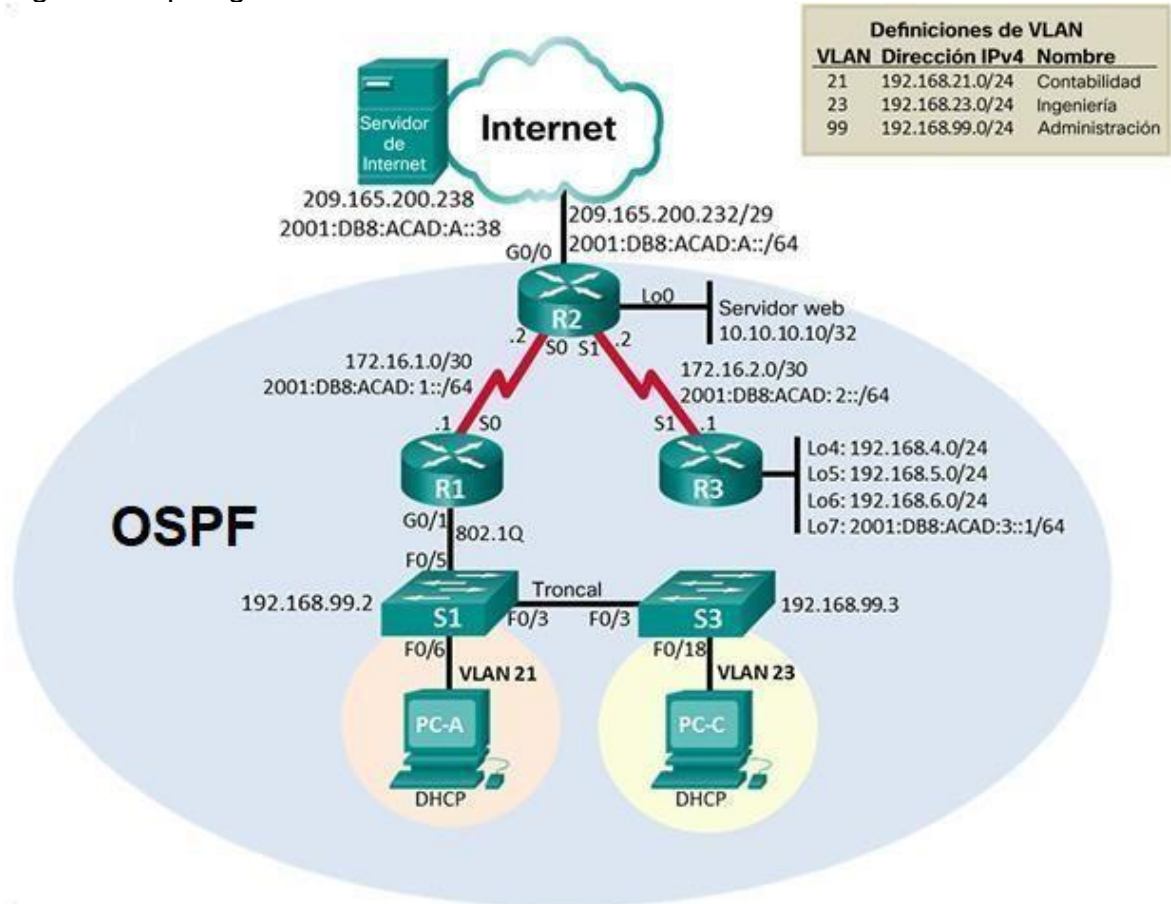
Tabla 4 Información PC-B

PC-B Network Configuration	
Descripción	PC-B para 50 host
Dirección física	00E0.F79E.23DC
Dirección IP	192.168.13.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.13.128

Fuente: Autor

2. Escenario 2

Figura 5 Topología escenario 2

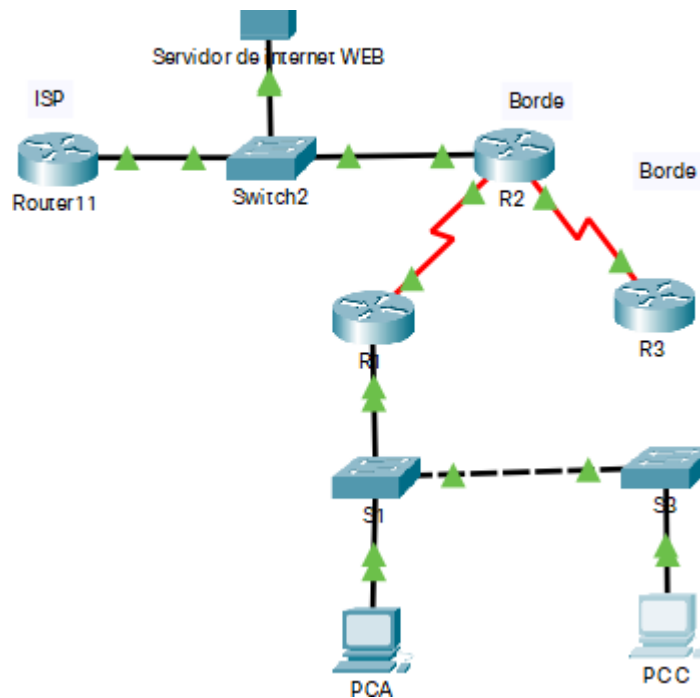


Fuente: Autor

Para el desarrollo del segundo escenario de la prueba de habilidades de CCNA, se realiza el montaje de los diferentes dispositivos en el simulador Cisco packet tracer.

Para el desarrollo práctico de esta actividad se efectúan algunas variaciones sobre la topología base que permitirá un desarrollo más práctico y con solución a errores. A continuación, se muestra la topología implementada para esta actividad.

Figura 6 Topología 2 en packet tracer



Fuente: Autor

2.1 Inicializar los dispositivos.

Se elimina la configuración de inicio de todos los dispositivos en la red con la ayuda del comando **erase startup-config**

Tabla 5 Eliminación de configuración de inicio

Tarea	Comando
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers. Configuración aplicada a:	R1, R2, R3, S1, S3, Switch 2, Router 11

Fuente: Autor

2.2.1 Configurar parámetros básicos de los dispositivos

Tabla 6 Parámetros de configuración

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::238
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Autor

Se configuran los parámetros descritos anteriormente en el SERVIDOR DE INTERNET WEB de la topología de red presentada en cisco packet tracer.

2.2.2 Configurar R1

A continuación, se describe el código utilizado para realizar la configuración inicial en los router junto con una breve explicación de los comandos más relevantes. tomando como guía la prueba de habilidades CISCO CCNA.

```
R1
Router>enable                               Modo exced privilegiado
Router#configure terminal                   Modo de configuración
Router(config)#no ip domain-lookup         Desactiva la búsqueda DNS
Router(config)#hostname R1                 Se establece el nombre del
                                           router como R1
R1(config)#enable secret class             Contraseña para exec
                                           privilegiado
R1(config)#line console 0                  contraseña para la consola
R1(config-line)#password cisco
R1(config-line)#login

R1(config-line)#line vty 0 4               Contraseña para acceso de
R1(config-line)#password cisco             telnet
R1(config-line)#login

R1(config-line)#exit
```

R1(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
R1(config)#banner motd "se prohíbe el acceso no autorizado"	Mensaje de restricción de ingreso
R1(config)#ipv6 unicast-routing	Permite el enrutamiento de ip versión 6
R1(config)#int s0/2/0	ingreso a la interfaz s0/2/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252	Asignación de dirección ip
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64	Asignación de dirección ipv6
R1(config-if)#clock rate 128000	Frecuencia de reloj
R1(config-if)#no shutdown	encender la interfaz
R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0	Configuración de ruta predeterminada ipv4
R1(config)#ipv6 route ::/0 S0/2/0	Configuración de ruta predeterminada ipv6

2.2.3 Configuración R2

Línea de comandos para la configuración de los parámetros básicos en R2

R2	
Router(config)#no ip domain-lookup	Desactivar la búsqueda DNS
R2(config)#hostname R2	Nombre a router como R2
R2(config)#enable secret class	Contraseña para exec privilegiado
R2(config)#line console 0	contraseña para la consola
R2(config-line)#password cisco	
R2(config-line)#login	
R2(config-line)#line vty 0 4	
R2(config-line)#password cisco	Contraseña para acceso de telnet
R2(config-line)#login	
R2(config-line)#exit	
R2(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
R2(config)#banner motd "se prohíbe el acceso no autorizado"	Mensaje de restricción de ingreso

R2(config)#ipv6 unicast-routing	Permite el enrutamiento de ip versión 6
R2(config)#int s0/2/0	ingreso a la interfaz s0/2/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252	Asignación de dirección ip
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64	Asignación de dirección ipv6
R2(config-if)#no shutdown	encender la interfaz
R2(config)#int s0/2/1	ingreso a la interfaz s0/2/0
R2(config-if)#ip address 172.16.2.1 255.255.255.252	Asignación de dirección ip
R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64	Asignación de dirección ipv6
R2(config-if)#clock rate 128000	Frecuencia de reloj
R2(config-if)#no shutdown	encender la interfaz
R2(config)#int G0/0/0	Ingreso a la interfaz G0/0/0
R2(config-if)#ip address 209.165.200.233 255.255.255.248	Asignación de dirección ip
R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64	Asignación de dirección ipv6
R2(config-if)#no shutdown	encender la interfaz
R2(config)#int loopback 0	Interfaz loopback 0
R2(config-if)#description servidor WEB	Descripción de loopback
R2(config-if)#ip address 10.10.10.10 255.255.255.255	Asignación dirección ip
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0/0	Configuración de ruta predeterminada ipv4
R2(config)#ipv6 route ::/0 G0/0/0	Configuración de ruta predeterminada ipv6

2.2.4 Configuraciones básicas en R3

A continuación, se presentan los comandos de configuración básica para el router R3.

R3	
Router>enable	Modo exec privilegiado
Router#configure terminal	Modo de configuración global
Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS
Router(config)#hostname R3	Asigna nombre R3
R3(config)#enable secret class	Contraseña para exec privilegiado
R3(config)#line console 0	contraseña para la consola
R3(config-line)#password cisco	
R3(config-line)#login	
R3(config-line)#line vty 0 4	Contraseña para acceso de telnet
R3(config-line)#password cisco	
R3(config-line)#login	
R3(config-line)#exit	Salir
R3(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
R3(config)#banner motd "se prohíbe el acceso no autorizado"	Mensaje de restricción de ingreso
R3(config)#ipv6 unicast-routing	Permite el enrutamiento de ip versión 6
R3(config)#int s0/2/1	Ingreso a la interfaz S0/2/0
R3(config-if)#ip address 172.16.2.2 255.255.255.252	Asignación de dirección ipv4
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64	Asignación de dirección ipv6
R3(config-if)#no shutdown	Encender la interfaz
R3(config)#int loopback 4	Se establece la loopback 4
R3(config-if)#ip add 192.168.4.1 255.255.255.0	se asigna la dirección ipv4 a la loopback 4
R3(config-if)#exit	salir
R3(config)#int loopback 5	Se establece la loopback 5
R3(config-if)#ip add 192.168.5.1 255.255.255.0	se asigna la dirección ipv4 a la loopback 5
R3(config-if)#exit	salir
R3(config)#int loopback 6	Se establece la loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0	se asigna la dirección ipv4 a la loopback 6
R3(config-if)#exit	salir

R3(config)#interface loopback 7	Se establece la loopback 7
R3(config-if)#ipv6 address	se asigna la dirección ipv6 a la
2001:DB8:ACAD:3::1/64	loopback 7
R3(config-if)#exit	salir
R3(config)#ip route 0.0.0.0 0.0.0.0 S0/2/1	Configuración de ruta
	predeterminada ipv4
R3(config)#ipv6 route ::/0 S0/2/1	Configuración de ruta
	predeterminada ipv6

2.2.5 Configuración en S1

Línea de comando para configuración en S1.

S1	
Switch#configure terminal	Modo de configuración global
Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNA
Switch(config)#hostname S1	Nombre de switch S1
S1(config)#enable secret class	Contraseña para exec
	privilegiado
S1(config)#line console 0	contraseña para la consola
S1(config-line)#password cisco	
S1(config-line)#login	
S1(config-line)#exit	
S1(config)#line vty 0 15	Contraseña para acceso de
S1(config-line)#password cisco	telnet
S1(config-line)#login	
S1(config)#service password-encryption	Cifrar las contraseñas de texto
	no cifrado
S1(config)#banner motd "se prohíbe el acceso	Mensaje de restricción de
no autorizado"	ingreso

2.2.6 Configuración en S3

S3	
Switch#configure terminal	Modo de configuración global

Switch(config)#no ip domain-lookup	Desactivar la búsqueda DNA
Switch(config)#hostname S3	Nombre de switch S3
S1(config)#enable secret class	Contraseña para exec privilegiado
S3(config)#line console 0	contraseña para la consola
S3(config-line)#password cisco	
S3(config-line)#login	
S3(config-line)#exit	
S3(config)#line vty 0 15	Contraseña para acceso de telnet
S3(config-line)#password cisco	
S3(config-line)#login	
S3(config)#service password-encryption	Cifrar las contraseñas de texto no cifrado
S3(config)#banner motd "se prohíbe el acceso no autorizado"	Mensaje de restricción de ingreso

2.2.7 Verificar la conectividad de red.

Una vez configurados los aspectos básicos en cada dispositivo, se precede a verificar la conectividad entre los mismos, para ello se realiza uso del comando ping entre las diferentes rutas propuestas en la siguiente tabla.

Tabla 7 Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	Correcto
R2	R3, S0/2/1	172.16.2.2	Correcto
PC de Internet	Gateway predeterminado	209:165:200:238	Correcto

Fuente: Autor

Adicionalmente, se comparte la captura de pantalla de cada uno de los pings realizados.

Figura 8 Ping de R1 a S0/2/0 de R2

```
R1>enable
Password:
R1#ping 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 = 1/5/12 ms

R1#
```

Fuente: Autor

Figura 7 Ping de R2 a S0/2/0 de R3

```
R2>enable
Password:
R2#ping 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 = 1/4/5 ms

R2#
```

Fuente: Autor

Figura 9 Ping de PC de internet a Gateway predeterminado

```
C:\>PING 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time=3ms TTL=128
Reply from 209.165.200.238: bytes=32 time=7ms TTL=128
Reply from 209.165.200.238: bytes=32 time=7ms TTL=128
Reply from 209.165.200.238: bytes=32 time=8ms TTL=128

Ping statistics for 209.165.200.238:
```

Fuente: Autor

2.3.0 Configuración de seguridad en el switch, VLAN y routing entre VLAN.

2.3.1 Configuración en S1

En este apartado se demuestra el código utilizado para realizar las tareas de configuración de VLAN en S1.

S3

S1(config)#vlan 21	Crear VLAN 21
S1(config-vlan)#name contabilidad	Nombre de vlan

S1(config-vlan)#vlan 23	Crear VLAN 23
S1(config-vlan)#name ingenieria	Nombre de vlan
S1(config-vlan)#vlan 99	Crear VLAN 99
S1(config-vlan)#name administracion	Nombre de vlan
S1(config)#int vlan 99	Ingreso a la VLAN de administración
S1(config-if)#ip add 192.168.99.2 255.255.255.0	Se asigna la dirección ipv4 a la VLAN de administración
S1(config-if)#no shutdown	Se enciende la interfaz
S1(config-if)#exit	Comando para salir
S1(config)#ip default-gateway 192.168.99.1	Asignación del gateway predeterminado
S1(config)#int f0/3	Ingreso a la interfaz F0/3
S1(config-if)#sw mode trunk	Configuración de puerto como enlace troncal
S1(config-if)#switchport trunk native vlan 1	Se utiliza la VLAN 1 como nativa
S1(config)#int f0/5	Ingreso a la interfaz F0/5
S1(config-if)#sw mode trunk	Configuración de puerto como enlace troncal
S1(config-if)#switchport trunk native vlan 1	Se utiliza la VLAN 1 como nativa
S1(config-if)#exit	Comando salir
S1(config)#interface range f0/1-2, f0/4, f0/7-24	Selección de puertos mediante un rango establecido
S1(config-if-range)#sw mode access	Se establecen los puertos de acceso
S1(config-if-range)#exit	Salir
S1(config-if)#int f0/6	Ingreso interfaz F0/6
S1(config-if)#sw mode access	
S1(config-if)#sw access vlan 21	Se asigna la interfaz a la VLAN 21
S1(config)#interface range f0/1-2, f0/4, f0/7-24	Selección de puertos mediante un rango establecido
S1(config-if-range)#shutdown	Se apagan los puertos

2.3.2 Configuración en S3

S3	
S3(config)#vlan 21	Crear VLAN 21
S3(config-vlan)#name contabilidad	Nombre de vlan
S3(config-vlan)#vlan 23	Crear VLAN 23
S3(config-vlan)#name ingenieria	Nombre de vlan
S3(config-vlan)#vlan 99	Crear VLAN 99
S3(config-vlan)#name administracion	Nombre de vlan
S3(config-vlan)#exit	Salir
S3(config)#int vlan 99	Ingreso a la VLAN de administración
S3(config-if)#ip add 192.168.99.3 255.255.255.0	Se asigna la dirección ipv4 a la VLAN de administración
S3(config-if)#no shutdown	Se enciende la interfaz
S3(config-if)#exit	Comando para salir
S3(config)#ip default-gateway 192.168.99.1	Asignación del gateway predeterminado
S3(config)#int f0/3	Ingreso a la interfaz F0/3
S3(config-if)#sw mode trunk	Configuración de puerto como enlace troncal
S3(config-if)#sw trunk native vlan 1	Se utiliza la VLAN 1 como nativa
S3(config)#int range f0/1 - f0/2	Selección de puertos mediante un rango establecido
S3(config-if-range)#sw mode access	Se establecen los puertos de acceso
S3(config-if-range)#int ran f0/7 - f0/24	Selección de puertos mediante un rango establecido
S3(config-if-range)#sw mode access	Se establecen los puertos de acceso
S3(config-if-range)#exit	Salir
S3(config)#int f0/18	Ingreso a la interfaz F0/18
S3(config-if)#sw acc vlan 21	Se asigna la interfaz a la VLAN 21
S3(config)#int range f0/7 - f0/17	Selección de puertos mediante un rango establecido
S3(config-if-range)#shudown	Se apagan los puertos

2.3.3 Configuración R1

```

R1
R1(config)#int g0/0/1
R1(config-if)#no shutdown

R1(config)#int g0/0/1.21

R1(config-subif)#description Lan contabilidad
R1(config-subif)#enc dot1q 21
R1(config-subif)#ip address 192.168.21.1
255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0/1.23

R1(config-subif)#desc Lan ingenieira
R1(config-subif)#en dot1q 23
R1(config-subif)#ip add 192.168.23.1
255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0/1.99

R1(config-subif)#description LAN administracion
R1(config-subif)#en dot1q 99
R1(config-subif)#ip add 192.168.99.1
255.255.255.0
R1(config-subif)#exit

```

Ingreso interfaz G0/0/1
Se enciende primero la interfaz para evitar errores de configuración
Configuración subinterfaz .21
Descripción en contabilidad
Se realiza la encapsulación
Se asigna la ipv4
salir
Configuración subinterfaz .23
Descripción en contabilidad
Se realiza la encapsulación
Se asigna la ipv4
salir
Configuración subinterfaz .99
Descripción en contabilidad
Se realiza la encapsulación
Se asigna la ipv4
salir

2.3.4 Pruebas de conectividad de red.

Como se indica en la guía de prueba de habilidades de cisco CCNA, con la ayuda del comando ping, se comprueba la conectividad entre los dispositivos de acuerdo con la siguiente tabla.

Tabla 8 Prueba de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLA 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	Correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto

S3	R1, dirección VLAN 23	192.168.23.1	Correcto
----	-----------------------	--------------	----------

Fuente: Autor

Se anexan las pantallas de comprobación de ping.

Figura 10 Ping de S3 a Vlan 23

```
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 = 0/0/2 ms

S3#
```

Fuente: Autor

Figura 11 Pin de S1 a Vlan 99

```
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

S1#
```

Fuente: Autor

Figura 12 Ping de S3 a Vlan 99

```
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#
```

Fuente: Autor

Figura 13 Ping de S1 a Vlan 21

```
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 = 0/1/8 ms

S3#
```

Fuente: Autor

2.4.0 Configuración de protocolo de routing dinámico OSPF

2.4.1 Configuración OSPF en R1

```
R1
R1(config)#router OSPF 13           Se asigna la OSPF
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0  Se anuncian la red conectadas
                                                                directamente
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#passive-interface g0/0/1           Se establecen las interfaces LAN
R1(config-router)#passive-interface g0/0/1.21       como pasivas
R1(config-router)#passive-interface g0/0/1.23
R1(config-router)#passive-interface g0/0/1.99
```

Nota: La tabla de configuración OSPF en R1 establece que se debe desactivar la somatización automática. Función que no se puede implementar en cisco packet tracer.

2.4.2 Configuración OSPF en R2

```
R2(config)#router ospf 13           Configuración OSPF
R2(config-router)#net 10.10.10.10 0.0.0.0 area 0  Se anuncian la red conectadas
                                                                directamente
R2(config-router)#net 172.16.1.0 0.0.0.3 area 0
R2(config-router)#net 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passive-interface loopback 0     Se establecen la interfaz loopback
                                                                como pasiva
```

Nuevamente no es posible desactivar la sumarizacion automática.

2.4.3 Configuración OSPFv3 EN R3

```
R3(config)#ipv6 router ospf 2          OSPF3
R3(config-rtr)#passive-interface lo 4  Se establecen las interfaces pasivas
R3(config-rtr)#passive-interface lo 5
R3(config-rtr)#passive-interface lo 6
```

2.4.4 Verificar la información de OSPF

A continuación, se da solución a las preguntas establecidas sobre OSPF si los comandos adecuados.

Figura 14 Comandos OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF,	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la	Show running

Fuente: Autor

Seguidamente se muestran las respuestas de los comandos anteriormente mencionados en R2

Figura 15 Comando Show ip protocols

```
R2>enable
Password:
R2#show ip protocols

Routing Protocol is "ospf 13"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
  10.10.10.10             110          00:01:02
  192.168.99.1            110          00:01:02
  Distance: (default is 110)

R2#
```

Fuente: Autor

Figura 16 Comando Show ip route ospf

```
R2#Show ip route ospf
O   192.168.21.0 [110/65] via 172.16.1.1, 00:02:13, Serial0/2/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:02:13, Serial0/2/0
R2#
```

Fuente: Autor

Figura 17 Comando Show running

```
router ospf 13
 log-adjacency-changes
 passive-interface Loopback0
 network 10.10.10.10 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
```

Fuente: Autor

2.5.0 Implementación de DHCP y NAT para IPv4

2.5.1 Configuración de R1 como servidor de DHCP para las Vlan 21 y 23

R1

R1#configure terminal

Modo de configuración

R1(config)#ip dhcp excluded-address
192.168.21.1 192.168.21.20

Se reservan las primeras direcciones en la Vlan 21

R1(config)#ip dhcp excluded-address
192.168.23.1 192.168.23.20

Se reservan las primeras direcciones en la Vlan 23

R1(config)#ip dhcp pool ACCT

Se crea el pool DHCP para la Vlan

R1(dhcp-config)#network 192.168.21.0
255.255.255.0

21 con nombre ACCT, servidor dns 10,10,10,10 y dominio. Se

R1(dhcp-config)#domain-name ccna-
sa.com

establece el gateway predeterminado

R1(dhcp-config)#dns-server 10.10.10.10

R1(dhcp-config)#default-router
192.168.21.1

R1(config)#ip dhcp pool ENGNR

Se crea el pool DHCP para la Vlan

R1(dhcp-config)#network 192.168.23.0
255.255.255.0

23 con nombre ENGNR, servidor dns 10,10,10,10 y dominio. Se

R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-
sa.com

establece el Gateway predeterminado

R1(dhcp-config)#default-router
192.168.23.1

2.5.2 Configuración de NAT estática y dinámica en R2

R2

R2(config)#username webuser privilege 15 password cisco12345	Se crea base de datos con usuario contraseña y privilegio
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233	Se crea la NAT estática al servidor web
R2(config)#interface g0/0/0	Se asignan interfaces internas y externas para la nat estática
R2(config-if)#ip nat outside	
R2(config-if)#int S0/2/0	
R2(config-if)#ip nat inside	
R2(config-if)#int s0/2/1	
R2(config-if)#ip nat inside	
R2(config-if)#int lo 0	
R2(config-if)#ip nat inside	
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255	Configuración de la NAT dinámica dentro de una red
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255	ACL privada
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255	
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.238 netmask 255.255.255.248	Define el pool de direcciones ip publicas utilizables
R2(config)#ip nat inside source list 1 pool INTERNET	Define la traducción de NAT dinámica

2.5.3 Verificar el protocolo DHCP y la NAT estática

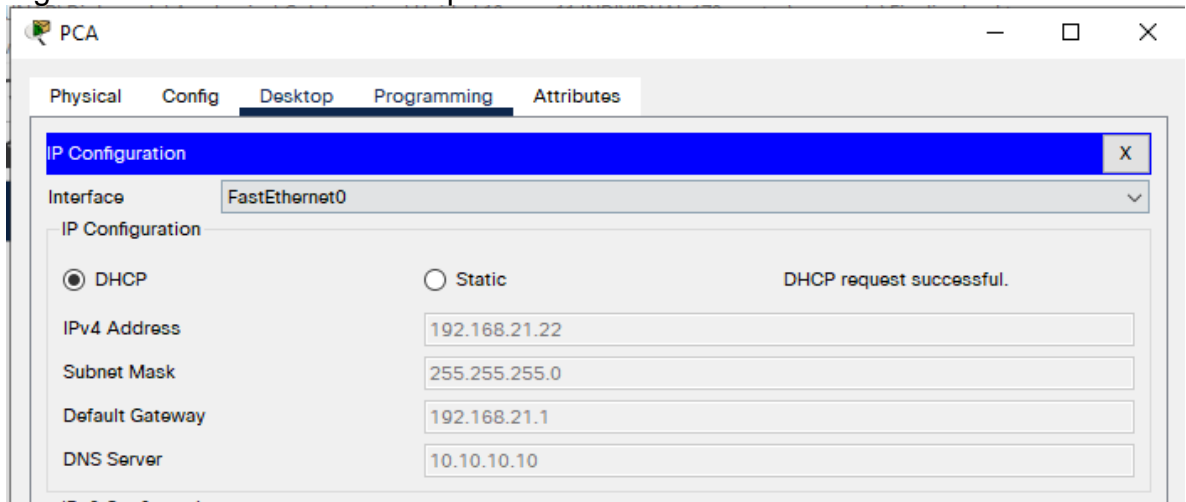
Tabla 9 Pruebas protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de	La computadora recibe la
Verificar que la PC-C haya adquirido información de	La computadora recibe la
Verificar que la PC-A pueda hacer ping a la PC-C	Correcto
Utilizar un navegador web en la computadora de Internet para acceder al servidor web	Se conecta correctamente

Fuente: Autor

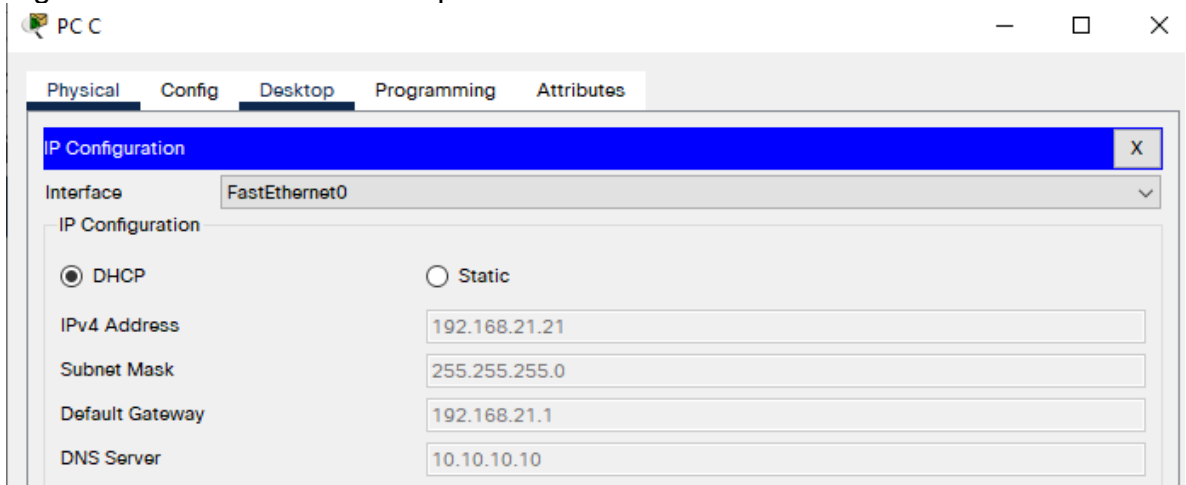
Se adjuntan las capturas de pantalla del proceso.

Figura 18 Dirección IP tomada por DHCP en PC-A



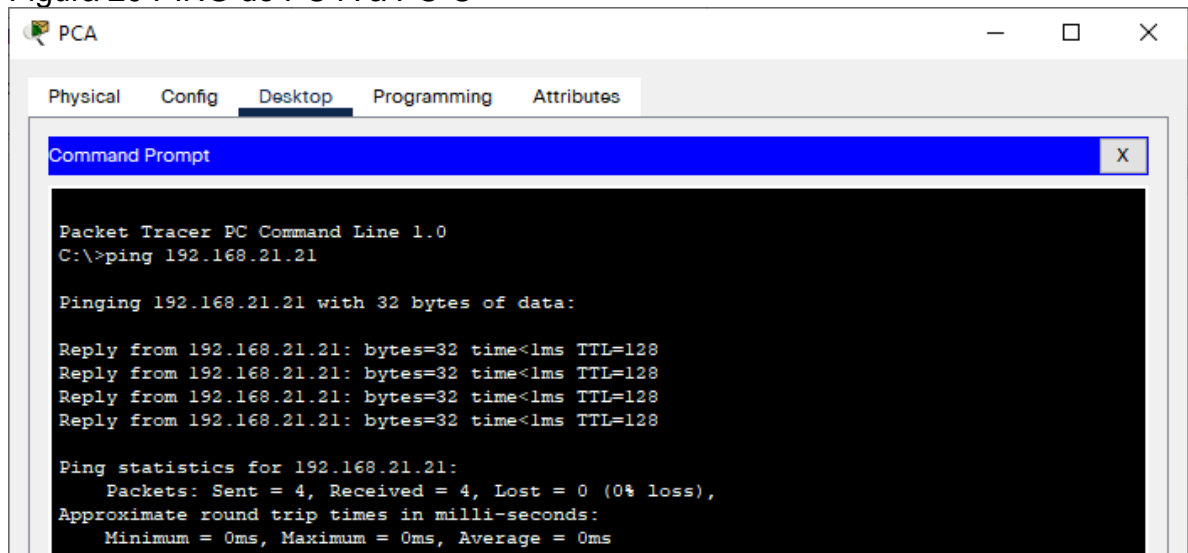
Fuente: Autor

Figura 19 Dirección IP tomada por DHCP en PC-C



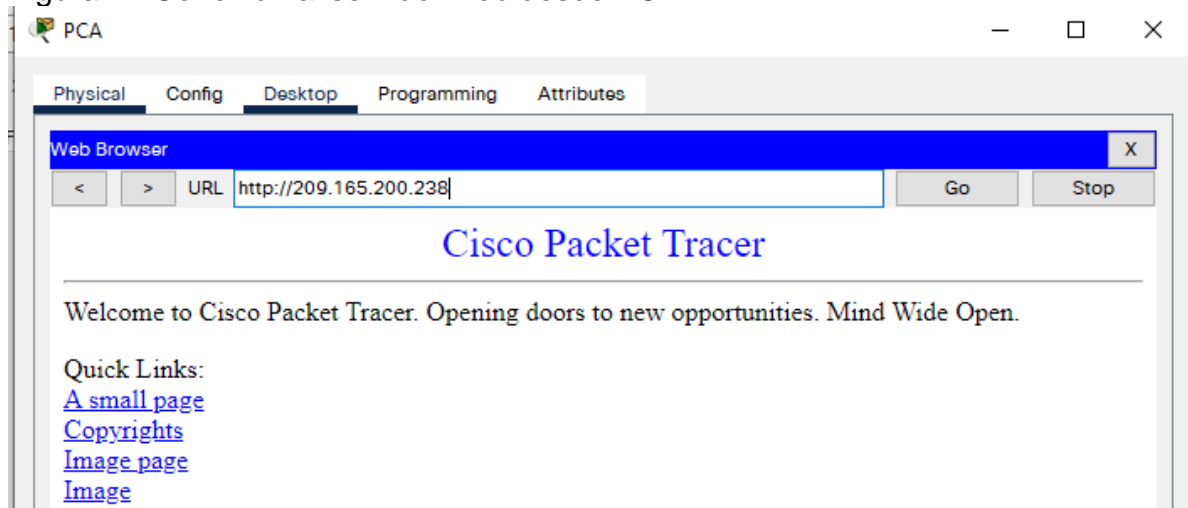
Fuente: Autor

Figura 20 PING de PC-A a PC-C



Fuente: Autor

Figura 21 Conexión al servidor web desde PC-A



Fuente: Autor

2.6.0 Configuración NTP

R2#clock set 09:00:00 05 march 2016

Configuración de fecha y hora

R2#config terminal

modo de configuración

R2(config)#ntp master 5	se configura R2 como maestro NTP
R2(config)#exit	
R1(config)#ntp server 172.16.1.2	Se configura R1 como cliente NTP
R1(config)#ntp update-calendar	Se solicita actualizaciones periódicas

2.7.0 Configuración de listas de acceso

2.7.1 Restringir el acceso a las líneas VTY en el R2

R2(config)#ip access-list standard ADMIN-MGT	Se configura lista de acceso con nombre ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1	
R2(config)#line vty 0 4	Aplica la ACL con nombre a las líneas VTY
R2(config-line)#ip access-class ADMIN-MGT in	
R2(config-line)#transport input telnet	Permite el acceso a telnet por las líneas VTY

2.7.2 Introducir el comando CLI adecuado en la siguiente tabla.

Tabla 10 Lista de comandos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de	Show Access-list
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se	show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las	Clear ip nat translation

Fuente: Autor

Figura 22 Comando Show access-list

```

R2#Show access-list
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1
 20 deny any
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255
 20 permit 192.168.5.0 0.0.0.255
 30 permit 192.168.6.0 0.0.0.255

```

Fuente: Autor

Figura 23 Comando show ip interface

```

show ip interface s0/2/0
Serial0/2/0 is up, line protocol is up (connected)
 Internet address is 172.16.1.2/30
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500
 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 unreachable 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
--More--

```

Fuente: Autor

Figura 24 Comando Show ip nat translations

```

R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.233    10.10.10.10      ---                ---
tcp 209.165.200.234:1025192.168.21.22:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1026192.168.21.22:1026 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.234:1027192.168.21.22:1027 209.165.200.238:80 209.165.200.238:80

```

Figura 25 Comando Clear ip nat translation

```

R2#Clear ip nat translation *
R2#
R2#show ip nat tr
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.233    10.10.10.10      ---                ---
R2#

```

Fuente: Autor

CONCLUSIONES

Es importante reconocer el trabajo que realiza la máscara de red para el diseño e implementación de subredes con direccionamiento IP versión 4, ya que de allí partirán criterios importantes como el tamaño de la red y subredes, número de host y direcciones IP disponibles para conectar.

Con el desarrollo del escenario número 1 de la prueba de habilidades prácticas, se lograron poner en práctica los conocimientos adquiridos en cada uno de los capítulos del curso de cisco, adicionalmente, se concientiza la importancia del correcto diseño de subredes mediante tablas y técnicas de direccionamiento, ya que en ellas se encuentra Core de la administración de redes de telecomunicaciones.

Al finalizar la presente actividad de desarrollo se evidencian situaciones en la simulación permite realizar el enrutamiento del router y switch conectado por el protocolo de red para el encaminamiento jerárquico de interior. Al avanzar en el desarrollo práctico se asignó las direcciones a los protocolos de internet (IP) a los diferentes equipos de conexión según lo proyectado en la guía de actividades

Para el desarrollo del segundo escenario, se encontraron los cambios en la comunicación hacia servidores y conexiones HTTP respecto al primer escenario.

Se lograron poner a prueba los conocimientos sobre temas de gran importancia en las redes como DHCP, OSPF y NAT. Se logra entender la utilidad que tienen para que las redes sean mas seguras, sencillas y eficientes.

BIBLIOGRAFÍA

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>

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>

CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2>

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3>

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm

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

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

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

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

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.

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.

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.

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

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.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, octubre). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-5). IEEE.

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 Ingeniería (CONIITI)* (pp. 1-6). IEEE.