

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS COPORATIVOSBAJO
EL USO DE TECNOLOGIA CISCO

JHON JAIRO MONTENEGRO MURILLO

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

CALI-VALLE

2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS COPORATIVOSBAJO EL
USO DE TECNOLOGIA CISCO

JHON JAIRO MONTENEGRO MURILLO

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

TUTOR:
NANCY AMPARO GUACA

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

CALI-VALLE

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

AGRADECIMIENTOS

A Dios que me brinda la oportunidad de perseverar en los objetivos planteados en mi vida, a mi familia que me han apoyado incondicionalmente en este proceso y a mi compañera de vida que me ha dado aliento para no desfallecer ante las dificultades y salir adelante con todo este proceso

TABLA DE CONTENIDO

AGRADECIMIENTOS	4
Tabla de contenido.....	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS.....	8
GLOSARIO.....	9
RESUMEN	10
ABSTRACT	11
INTRODUCCION	12
DESARROLLO.....	13
1.1 ESCENARIO 1.....	13
Objetivos	13
Aspectos básicos/situación	13
Parte 1: Construya la Red	13
Parte 2: Desarrolle el esquema de direccionamiento IP	13
Parte 3: Parte 3: Configure aspectos básicos	15
Paso 2. Configurar los equipos	18
1.2 ESCENARIO 2.....	28
Topología	28
Parte 1: Inicializar dispositivos.....	29
Paso 1: Inicializar y volver a cargar los routers y los switches.....	29
Parte 2: Configurar los parámetros básicos de los dispositivos	30
Paso 2: Configurar R1	31
Paso 3: Configurar R2	32
Paso 4: Configurar R3	33

Paso 5: Configurar S1.....	36
Paso 6: Configurar el S3.....	36
Paso 7: Verificar la conectividad de la red	37
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	
Paso 1: Configurar S1	42
Paso 2: Configurar el S3.....	44
Paso 3: Configurar R1	45
Paso 4: Verificar la conectividad de la red	47
Parte 4: Configurar el protocolo de routing dinámico OSPF.....	52
Paso 2: Configurar OSPF en el R2	52
Paso 3: Configurar OSPFv3 en el R2	53
Paso 4: Verificar la información de OSPF.....	53
Parte 5: Implementar DHCP y NAT para IPv4	55
Paso 2: Configurar la NAT estática y dinámica en el R2.....	56
Paso 3: Verificar el protocolo DHCP y la NAT estática	57
Parte 6: Configurar NTP	63
Paso 1: Restringir el acceso a las líneas VTY en el R2	63
CONCLUSIONES.....	66
BIBLIOGRAFIA	67

LISTA DE TABLAS

Tabla 1: Direccionamiento.....	14
Tabla 2 Subneteo.....	15
Tabla 3: Configuración de aspectos básicos.....	15
Tabla 4: Configuración del S1.....	17
Tabla 5: Configuración de PC-A.....	18
Tabla 6: Configuración PC-B.....	19
Tabla 8: Configuración del servidor de internet.....	30
Tabla 9: Configuración de R1.....	31
Tabla 10: Configuración de R2.....	32
Tabla 11: Configuración de R3.....	33
Tabla 12: Configuración de S1.....	36
Tabla 12: Configuración de S3.....	36
Tabla 13: Verificación de conectividad.....	37
Tabla 14: Configuración del S1 y VLAN.....	42
Tabla 15: Configuración de S3.....	44
Tabla 16: Configuración de R1.....	45
Tabla 17: Verificación de conectividad.....	47
Tabla 18: Configuración de OSPF en el R1.....	52
Tabla 19: Configuración de OSPF en el R2.....	52
Tabla 20: Configuración de OSPFv3 en el R2.....	53
Tabla 21: Verificación de información en OSPF.....	53
Tabla 22: Configuración del R1 servidor de DHCP para VLAN 21 y 23.....	55
Tabla 23: Configuración de NAT estática y dinámica en el R2.....	56
Tabla 23: Configuración de NTP.....	63
Tabla 24: Restringir acceso líneas VTY en el R2.....	64
Tabla 25: Descripción de comandos.....	65

LISTA DE FIGURAS

Figura 1 Topología De Red	13
Figura 2 : Configuración ip estática PC A	20
Figura 3: Configuración ip estática PC B	21
Figura 4: Ping de PCA a PCB	22
Figura 5: Ping PCA a R1	23
Figura 6: Ping PCB a PCA	24
Figura 7: Ping PCB a R1	25
Figura 8: Comando Show ip interface y show arp	26
Figura 9: Show ip interface brief.....	27
Figura 10: Topología escenario 2.....	28
Figura 11: Topología en packet tracet.	29
Figura 12: Ping entre R1 y R2.....	38
Figura 13: Ping entre R2 y R3.....	39
Figura 14: Ping a servidor de internet	40
Figura 15: Ping desde server a ip .233	41
Figura 16: Ping desde S1 a R1 VLAN 99.....	49
Figura 17: Ping desde S3 a R1 VLAN 99.....	50
Figura 18: Ping desde S3 a R1 VLAN 23.....	51
Figura 19: Ping desde S1 a R1 Vlan 21	51
Figura 20: comando Show ip protocols	54
Figura 21: Comando para mostrar solo las rutas OSPF	55
Figura 22: Comando para mostrar la sección de OSPF.....	55
Figura 23: Verificar PC-A adquiere información IP del servidor DHCP	58
Figura 24: Verificar PC-C adquiere información IP servidor DHCP.....	59
Figura 25: Verificar que la PC-A realice ping a PC-C.....	60
Figura 26: Conectividad desde el PC-A hacia el servidor WEB	61
Figura 27: Conectividad PC-A hacia servidor WEB – Prueba de Ping.....	62
Figura 28: Verificación de NTP en R1	63
Figura 29: Verificar funcionamiento de ACL.....	64

GLOSARIO

- Subnetting:** Definido de la forma más simple, el término subnetting hace referencia a la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet
- IPv4:** Un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET. Definida en el RFC 791, el IPv4 usa direcciones de 32 bits.
- IPv6:** Es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.
- PACKET TRACERT:** Herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.
- ROUTER:** Dispositivo de hardware que permite la interconexión de ordenadores en red. Este dispositivo es el encargado de distribuir la conexión a Internet a distintos computadores vinculados a una misma red local actuando como un puente entre nuestros dispositivos y la internet

RESUMEN

En el presente trabajo se muestra el desarrollo de la prueba final de habilidades prácticas de CCNA del diplomado de profundización CISCO como requisito para optar al grado de Ingeniería de Sistemas de la Universidad Nacional Abierta y a Distancia – UNAD. Al desarrollar esta prueba cuyo tema principal era el diseño e implementación de soluciones integradas en redes LAN y WAN, se experimentó el papel que cumple un administrador de red en tareas de configuración e implementación de los diferentes elementos que conforman una red empresarial y de los recursos a utilizar.

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

ABSTRACT

This paper shows the development of the final CCNA practical skills test of the CISCO in-depth diploma as a requirement to qualify for the degree in Systems Engineering at the National Open and Distance University - UNAD. When developing this test whose main topic was the design and implementation of integrated solutions in LAN and WAN networks, the role of a network administrator in configuration and implementation tasks of the different elements that make up a business network and the resources was experienced. to use.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Systems

INTRODUCCION

Mediante la presente actividad, se realizarán dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados.

Para el segundo 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, y demás configuraciones que contribuyen a la correcta solución del escenario.

Finalmente, estará debidamente documentado y consta de una evidencia que determina la operación y aplicación de cada una de las instrucciones requeridas para el cumplimiento de lo solicitado en cada uno de los escenarios y además de verificar el funcionamiento y el comportamiento de la red a medida que se va implementando cada uno de los cambios y configuración de los dispositivos.

DESARROLLO

1.1 ESCENARIO 1

FIGURA 1 TOPOLOGÍA DE RED



Fuente: Prueba de habilidades CISCO CCNAII

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

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

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

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

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

Parte 2: Desarrolle el esquema de direccionamiento IP

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

Cada estudiante tomará el direccionamiento 192.168.82.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1: Direccionamiento

ITEM	REQUERIMIENTO
Dirección de Red	192.168.88.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.88.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.88.129/26
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.88.2/25
PC -A	Última dirección de host de la subred LAN1 192.168.88.126/25
PC -B	Última dirección de host de la subred LAN2 192.168.88.190/26

Fuente: Prueba de habilidades CISCO CCNAII

Tabla 2 Subneteo

L A N	N # H O S T	IP DE RED	MASCARA	HOST INICI AL	HOS T FIN AL	BROAD CAST
1	12 6	192.168.8 8 .0 / 25	255.255.25 5 .128	192.168.8 8 .1	192.168.8 8 .126	192.168.8 8 .127
2	62	192.168.8 8 .128 / 26	192.168.88 . 128	192.168.8 8 .129	192.168.8 8 .190	192.168.8 8 .191

Fuente: Prueba de habilidades CISCO CCNAII

Parte 3: Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3: Configuración de aspectos básicos

Tarea	Especificación
Desactivar la búsqueda DNS	R1(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)# domain-name ccna-lab.com
Contraseña cifrada para el modo EXECprivilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login

	R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)# security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#user admin privilege 15 secret admin1pass Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)# ip ssh version 2 R1(config)# line vty 0 15 R1(config-line)# login local R1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Configurar interfaz G0/0/0	R1(config)#interface Giga 0/0/0 R1(config-if)#description R1 a PCB R1(config-if)#ip address 192.168.88.129 255.255.255.192 R1(config-if)#no shutdown R1(config-if)#exit
Configurar interfaz G0/0/1	R1(config)#interface Giga 0/0/1 R1(config-if)#description R1 a S1 R1(config-if)#ip address 192.168.88.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)# crypto key generate rsa R1(config)#1024

Fuente: propia.

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4: Configuración del S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config))#hostname S1
Nombre de dominio	S1(config)# domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Tarea	Especificación
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#user admin privilege 15 secret admin1pass Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)# ip ssh version 2 S1(config)# line vty 0 15 S1(config-line)# login local S1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd

	#Se prohíbe el acceso no autorizado#
Generar una clave de cifrado RSA	S1(config)# crypto key generate rsa S1(config)#1024
Configurar la interfaz de administración (SVI)	S1(config)#vlan 1 S1 (config-vlan)#exit S1(config)#interface vlan 1 S1(config-if)#no shutdown S1(config-if)#ip address 192.168.88.2 255.255.255.128 S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.88.1

Fuente propia

Paso 2. Configurar los equipos

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

Tabla 5: Configuración de PC-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	00D0.FFAD.CBE5
Dirección IP	192.168.88.126
Máscara de subred	255.255.255.0
Gateway predeterminado	192.168.88.1

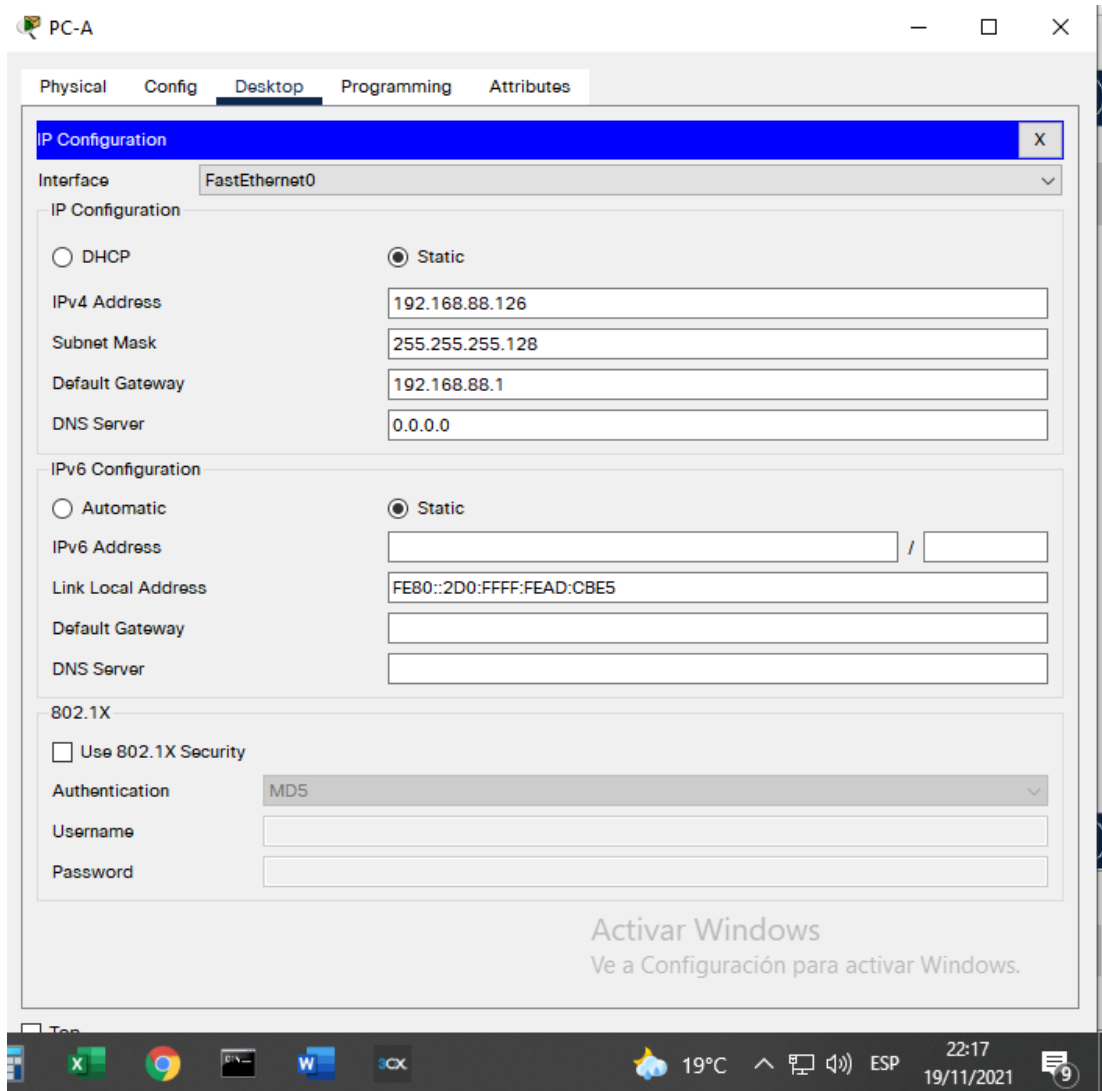
Fuente propia

Tabla 6: Configuración PC-B

PC-B Network Configuration	
Descripción	PC-B
Dirección física	00E0.8FC1.6E02
Dirección IP	192.168.88.190
Máscara de subred	255.255.255.0
Gateway predeterminado	192.168.88.1

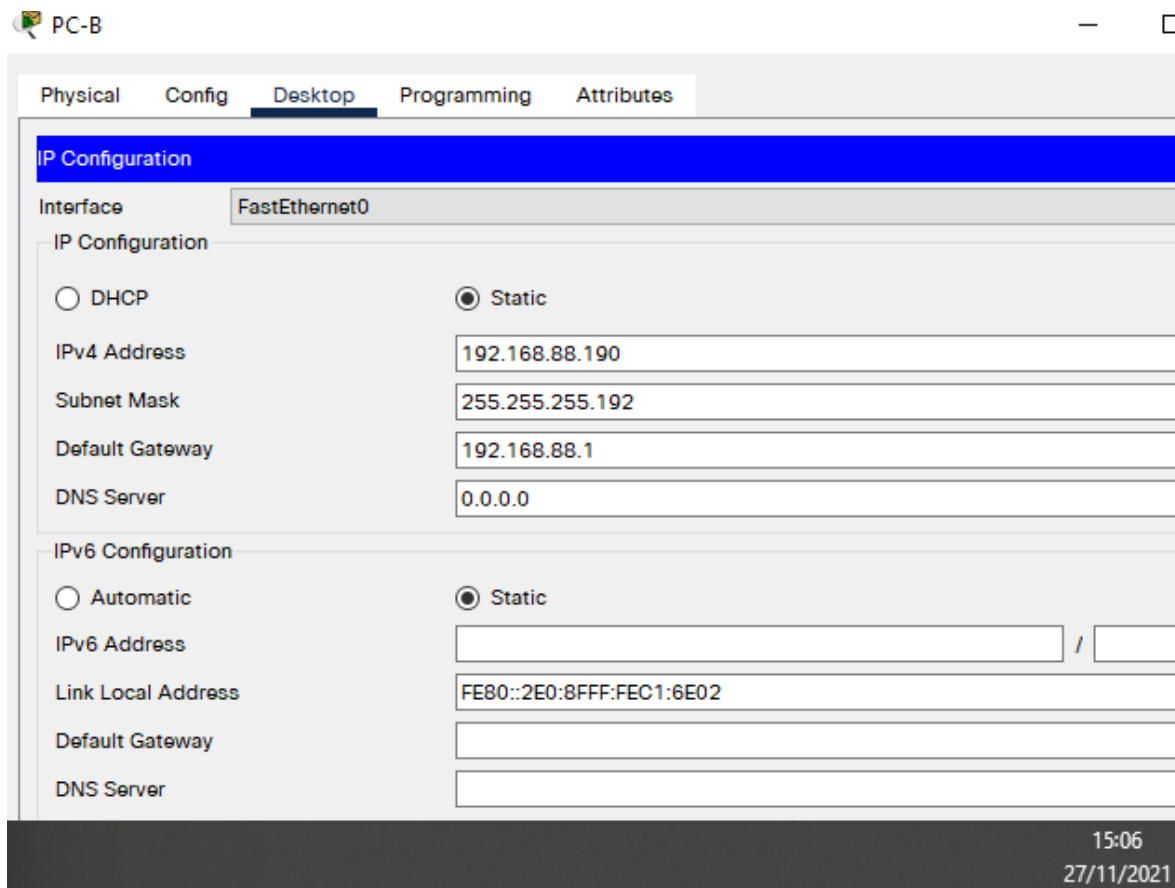
Fuente propia

Figura 2 : Configuración ip estática PC A



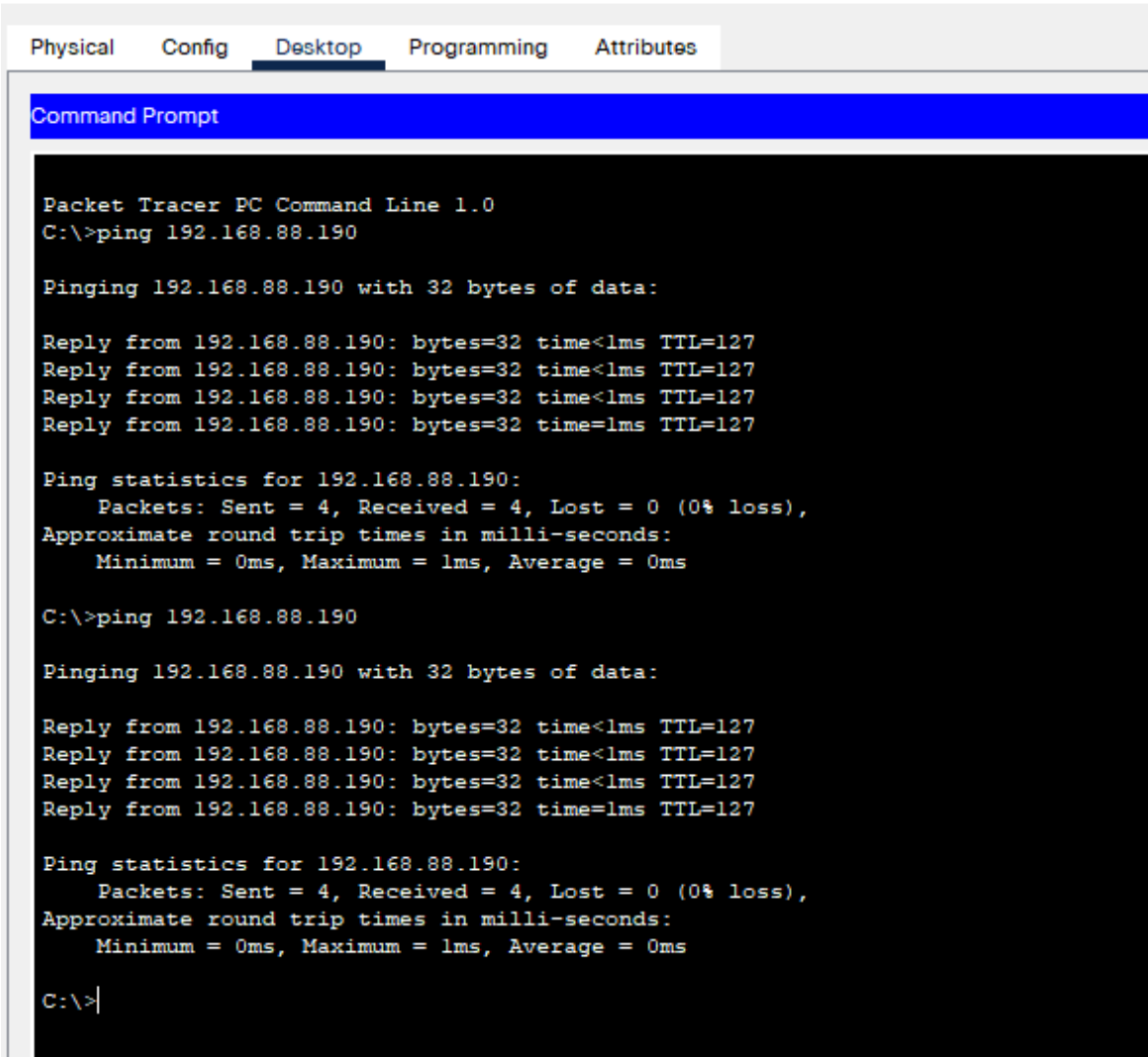
Fuente propia

Figura 3: Configuración ip estática PC B



Fuente propia.

Figura 4: Ping de PCA a PCB



The screenshot shows a Packet Tracer PC Command Line window for PC-A. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with Desktop selected. The Command Prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.88.190

Pinging 192.168.88.190 with 32 bytes of data:

Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time=lms TTL=127

Ping statistics for 192.168.88.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = lms, Average = 0ms

C:\>ping 192.168.88.190

Pinging 192.168.88.190 with 32 bytes of data:

Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time<lms TTL=127
Reply from 192.168.88.190: bytes=32 time=lms TTL=127

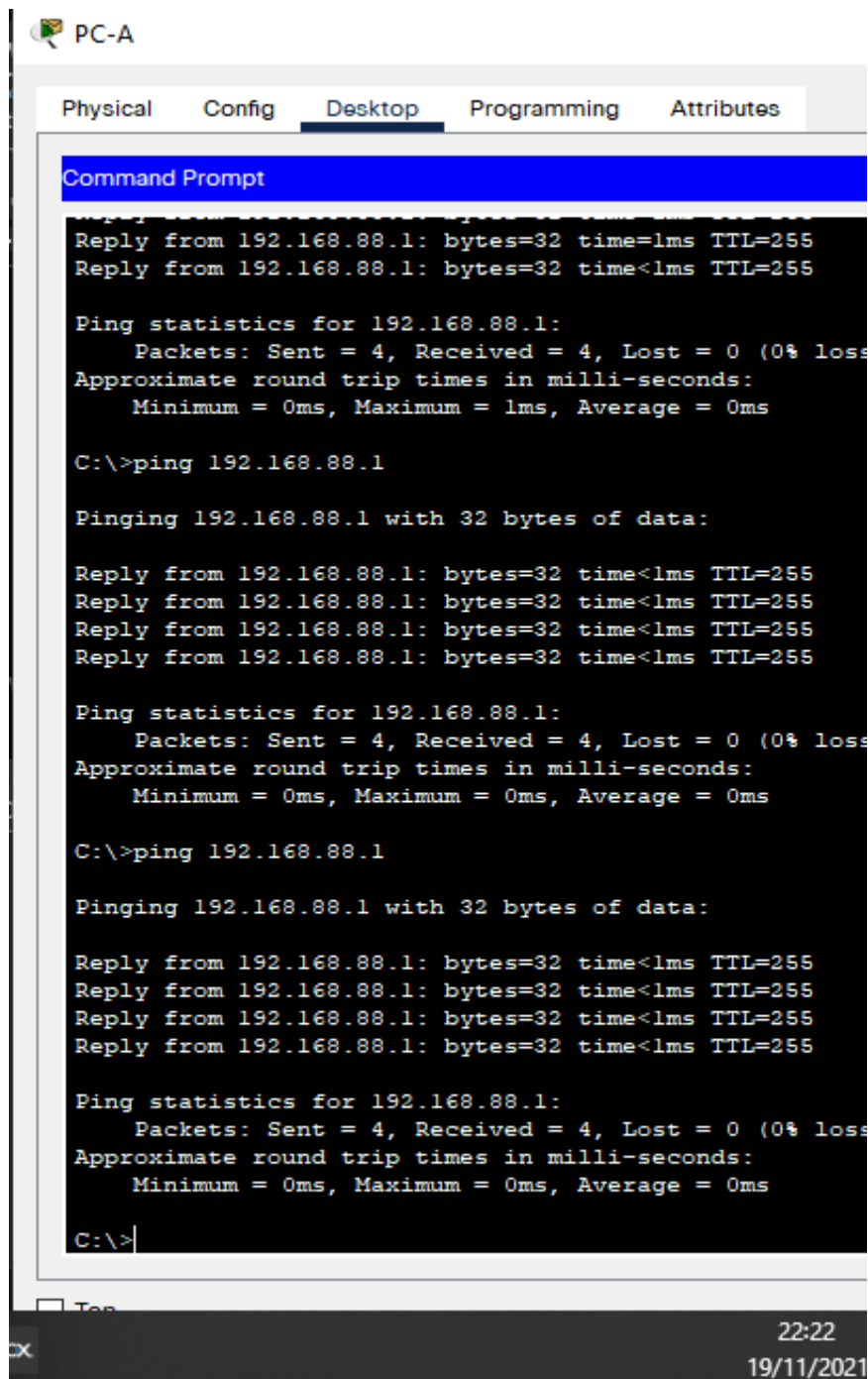
Ping statistics for 192.168.88.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = lms, Average = 0ms

C:\>|
```

The bottom right corner of the window displays the time 15:07 and the date 27/11/2021.

Fuente propia

Figura 5: Ping PCA a R1



The screenshot shows a Windows desktop environment for PC-A. The 'Desktop' tab is active in the top navigation bar. A Command Prompt window is open, displaying the results of a ping command to the IP address 192.168.88.1. The output shows four successful replies with 0% loss and a round trip time of less than 1ms. The Command Prompt interface includes a title bar with 'Command Prompt' and a standard Windows taskbar at the bottom with the system clock showing 22:22 on 19/11/2021.

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.88.1: bytes=32 time=1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:

Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:

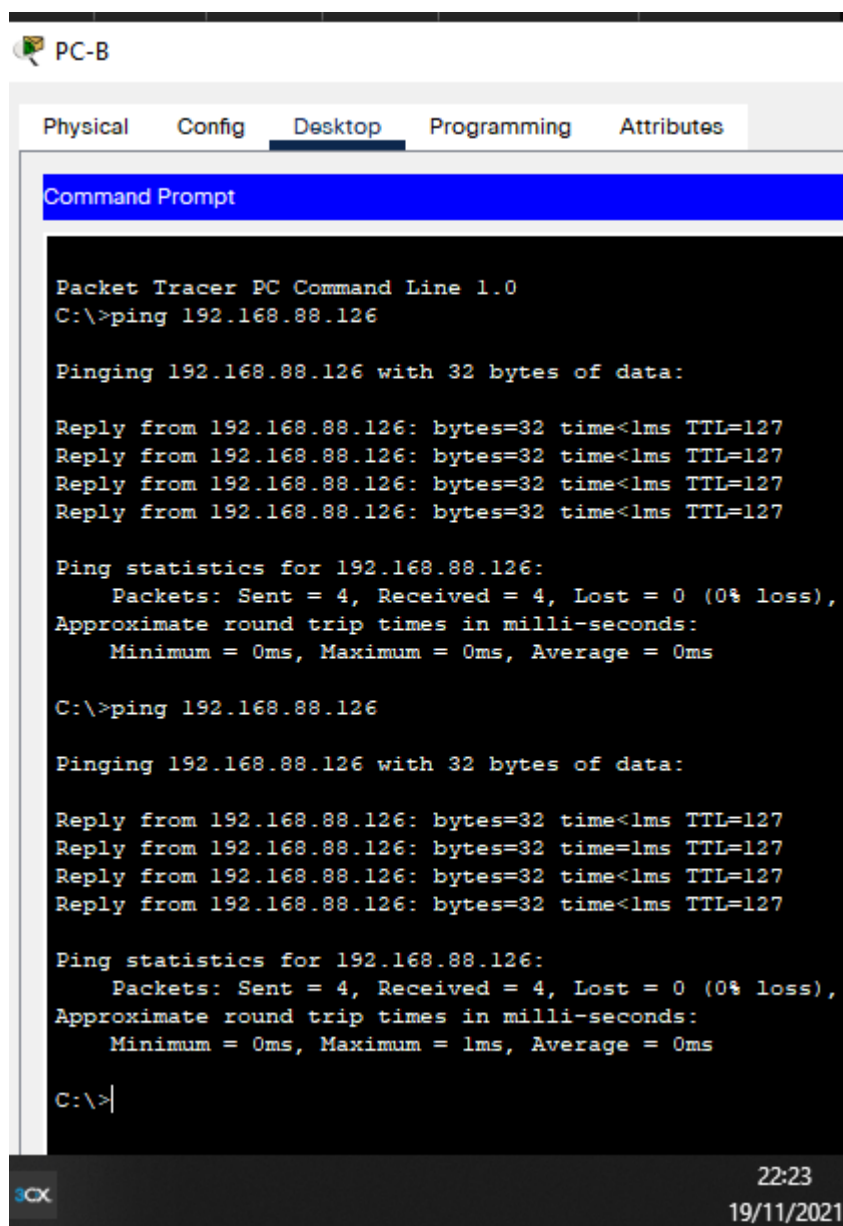
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255
Reply from 192.168.88.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente propia

Figura 6: Ping PCB a PCA



The screenshot shows a Packet Tracer interface for PC-B. The 'Desktop' tab is active, displaying a Command Prompt window. The prompt shows two successful ping operations to the IP address 192.168.88.126. Each operation shows four replies with 32 bytes of data, a time of 1ms, and a TTL of 127. The statistics for both operations indicate 0% loss, with a minimum, maximum, and average round trip time of 0ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.88.126

Pinging 192.168.88.126 with 32 bytes of data:

Reply from 192.168.88.126: bytes=32 time<1ms TTL=127
Reply from 192.168.88.126: bytes=32 time<1ms TTL=127
Reply from 192.168.88.126: bytes=32 time<1ms TTL=127
Reply from 192.168.88.126: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.88.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.88.126

Pinging 192.168.88.126 with 32 bytes of data:

Reply from 192.168.88.126: bytes=32 time<1ms TTL=127
Reply from 192.168.88.126: bytes=32 time=1ms TTL=127
Reply from 192.168.88.126: bytes=32 time<1ms TTL=127
Reply from 192.168.88.126: bytes=32 time<1ms TTL=127

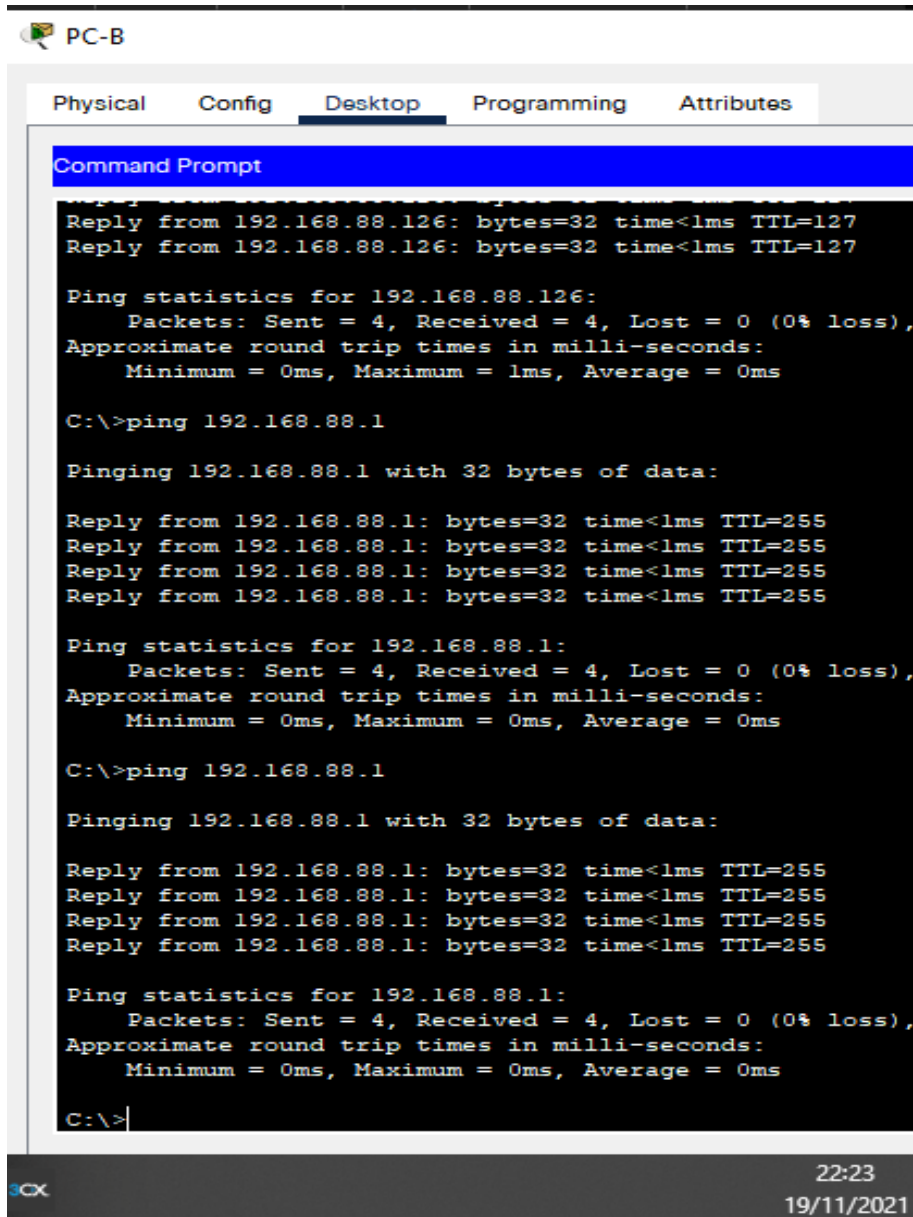
Ping statistics for 192.168.88.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

22:23
19/11/2021

Fuente propia

Figura 7: Ping PCB a R1



The screenshot shows a PC-B desktop environment with a Command Prompt window open. The window title is "Command Prompt". The desktop has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The Command Prompt shows the following output:

```
Reply from 192.168.88.126: bytes=32 time<lms TTL=127
Reply from 192.168.88.126: bytes=32 time<lms TTL=127

Ping statistics for 192.168.88.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:

Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:

Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255
Reply from 192.168.88.1: bytes=32 time<lms TTL=255

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

The system tray at the bottom right shows the time as 22:23 and the date as 19/11/2021.

Fuente propia

Figura 8: Comando Show ip interface y show arp

```
-----
R1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0/0 192.168.88.129 YES manual up          up
GigabitEthernet0/0/1 192.168.88.1   YES manual up          up
GigabitEthernet0/0/2 unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
R1#show ip arp
Protocol Address          Age (min) Hardware Addr  Type   Interface
Internet 192.168.88.1    -         0010.1183.E402  ARPA   GigabitEthernet0/0/1
Internet 192.168.88.2    7         0060.3E69.EEA3  ARPA   GigabitEthernet0/0/1
Internet 192.168.88.126  7         00D0.FFAD.CB55  ARPA   GigabitEthernet0/0/1
Internet 192.168.88.129  -         0010.1183.E401  ARPA   GigabitEthernet0/0/0
Internet 192.168.88.190  7         00E0.8FC1.6E02  ARPA   GigabitEthernet0/0/0
R1#
```

Ctrl+F6 to exit CLI focus

Copy

15:13

27/11/2021

Fuente propia

Figura 9: Show ip interface brief

```
Physical  Config  CLI  Attributes
IOS Command Line Interface
Password:
S1>ena
Password:
S1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    unassigned      YES manual  down        down
FastEthernet0/2    unassigned      YES manual  down        down
FastEthernet0/3    unassigned      YES manual  down        down
FastEthernet0/4    unassigned      YES manual  down        down
FastEthernet0/5    unassigned      YES manual  up          up
FastEthernet0/6    unassigned      YES manual  up          up
FastEthernet0/7    unassigned      YES manual  administratively down  down
FastEthernet0/8    unassigned      YES manual  administratively down  down
FastEthernet0/9    unassigned      YES manual  administratively down  down
FastEthernet0/10   unassigned      YES manual  administratively down  down
FastEthernet0/11   unassigned      YES manual  administratively down  down
FastEthernet0/12   unassigned      YES manual  administratively down  down
FastEthernet0/13   unassigned      YES manual  administratively down  down
FastEthernet0/14   unassigned      YES manual  administratively down  down
FastEthernet0/15   unassigned      YES manual  administratively down  down
FastEthernet0/16   unassigned      YES manual  administratively down  down
FastEthernet0/17   unassigned      YES manual  administratively down  down
FastEthernet0/18   unassigned      YES manual  administratively down  down
FastEthernet0/19   unassigned      YES manual  administratively down  down
FastEthernet0/20   unassigned      YES manual  administratively down  down
FastEthernet0/21   unassigned      YES manual  administratively down  down
FastEthernet0/22   unassigned      YES manual  administratively down  down
FastEthernet0/23   unassigned      YES manual  administratively down  down
FastEthernet0/24   unassigned      YES manual  administratively down  down
GigabitEthernet0/1 unassigned      YES manual  administratively down  down
GigabitEthernet0/2 unassigned      YES manual  administratively down  down
Vlan1              192.168.88.2    YES manual  up          up
Vlan10            192.168.88.10  YES manual  up          down
S1#
```

15:14
27/11/2021

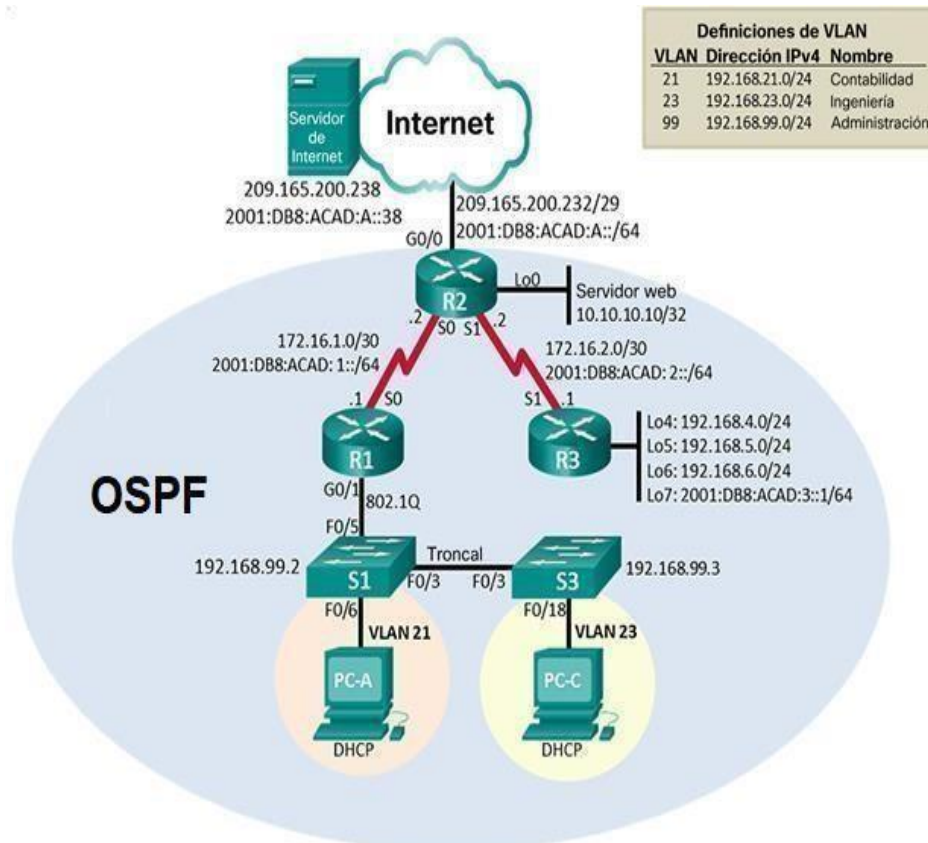
Fuente: Propia

1.2 ESCENARIO 2

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

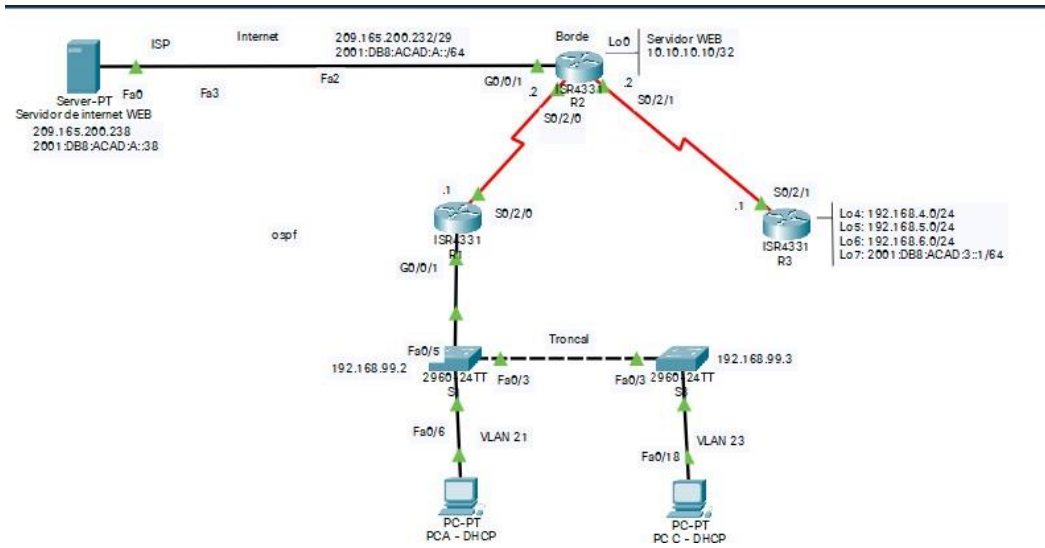
Topología

Figura 10: Topología escenario 2



Fuente: Prueba de habilidades CCNA II

Figura 11: Topología en packet tracert.



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 7: Inicializar y volver a cargar RT y SW

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	<pre>Router>enable Router#erase Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Router#</pre>
Volver a cargar todos los routers	<pre>Router#reload Proceed with reload? [confirm]</pre>
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	<pre>Switch>enable Switch#erase sta Switch#erase startup-config Erasing the nvram filesystem will</pre>

	remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4414921 <no date> c2960- lanbase-mz.122-25.FX.bin 64016384 bytes total (59601463 bytes free) Switch#

Fuente: Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: 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 8: Configuración del servidor de internet

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

Fuente: Propia

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9: 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 secret class
Contraseña de acceso a la consola	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/2/0	R1(config)#interface serial 0/2/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/2/0 R1(config)#ipv6 route ::/0 s0/2/0 R1(config)#ipv6 unicast R1(config)#ipv6 unicast-routing R1(config)#

Fuente: Propia

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10: Configuración de 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 secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/2/0	R2(config)#interface serial 0/2/0 R2(config-if)#description R2 a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit

Interfaz S0/2/1	<pre>R2(config)#interface serial 0/2/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#exit</pre>
Interfaz G0/0/1 (simulación de Internet)	<pre>R2(config)#interface gigabitEthernet 0/0/1 R2(config-if)#description R2 to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)# R2(config-if)#exit</pre>
Interfaz loopback 0 (servidor web simulado)	<pre>R2(config) #interface lo0 R2(config-if)# R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit</pre>
Ruta predeterminada	<pre>R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0/1 R2(config)#ipv6 route ::/0 gigabitEthernet 0/0/1 R2(config)#</pre>

Fuente: Propia

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11: Configuración de 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 con 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/2/1	R3(config)#interface serial 0/2/1 R3(config-if)#description R3 a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)# R3(config-if)#exit
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)# R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)# R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)# R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)# R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

	<pre>R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#</pre>
Rutas predeterminadas	<pre>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/2/1 R3(config)#ipv6 route ::/0 s0/2/1</pre>

Fuente: Propia

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12: Configuración de 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 secret class
Contraseña de acceso a la consola	S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Propia

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12: Configuración de 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 con 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco

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

Fuente: Propia

Paso 7: 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: Verificación de conectividad

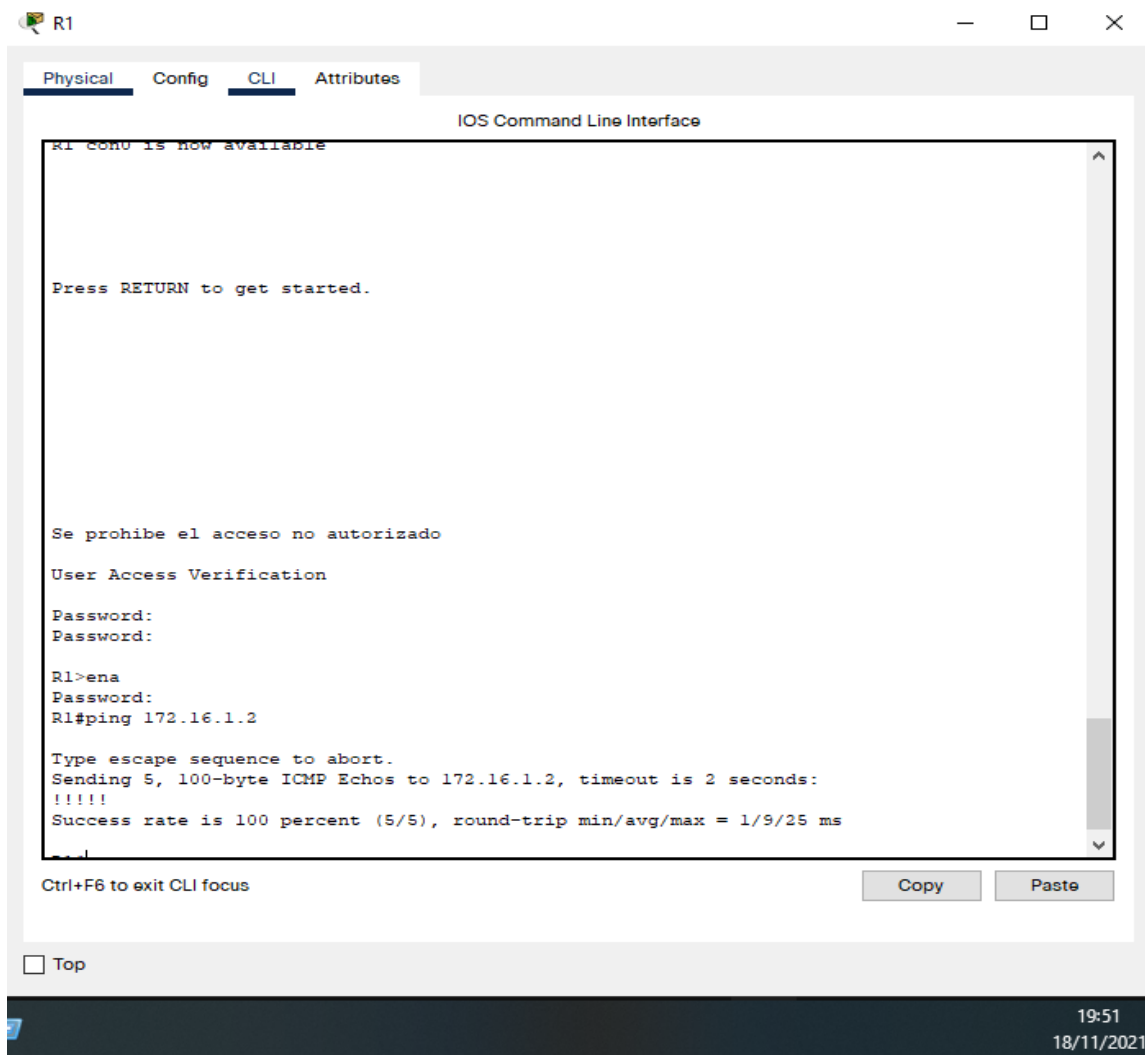
D e s d e	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/2/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/10 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 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 = 1ms, Average = 0ms
--	--	--	---

Fuente: Propia

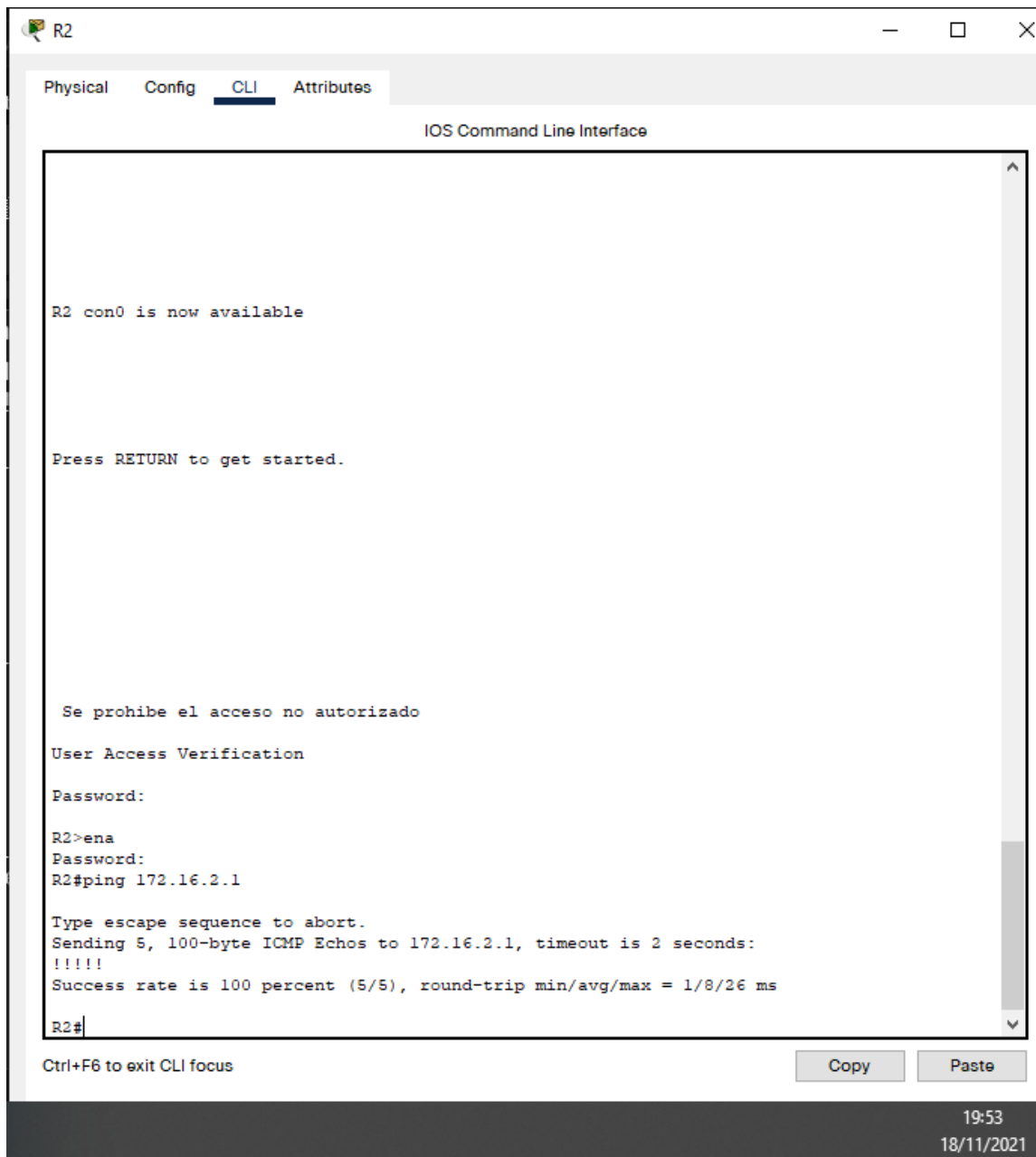
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 12: Ping entre R1 y R2



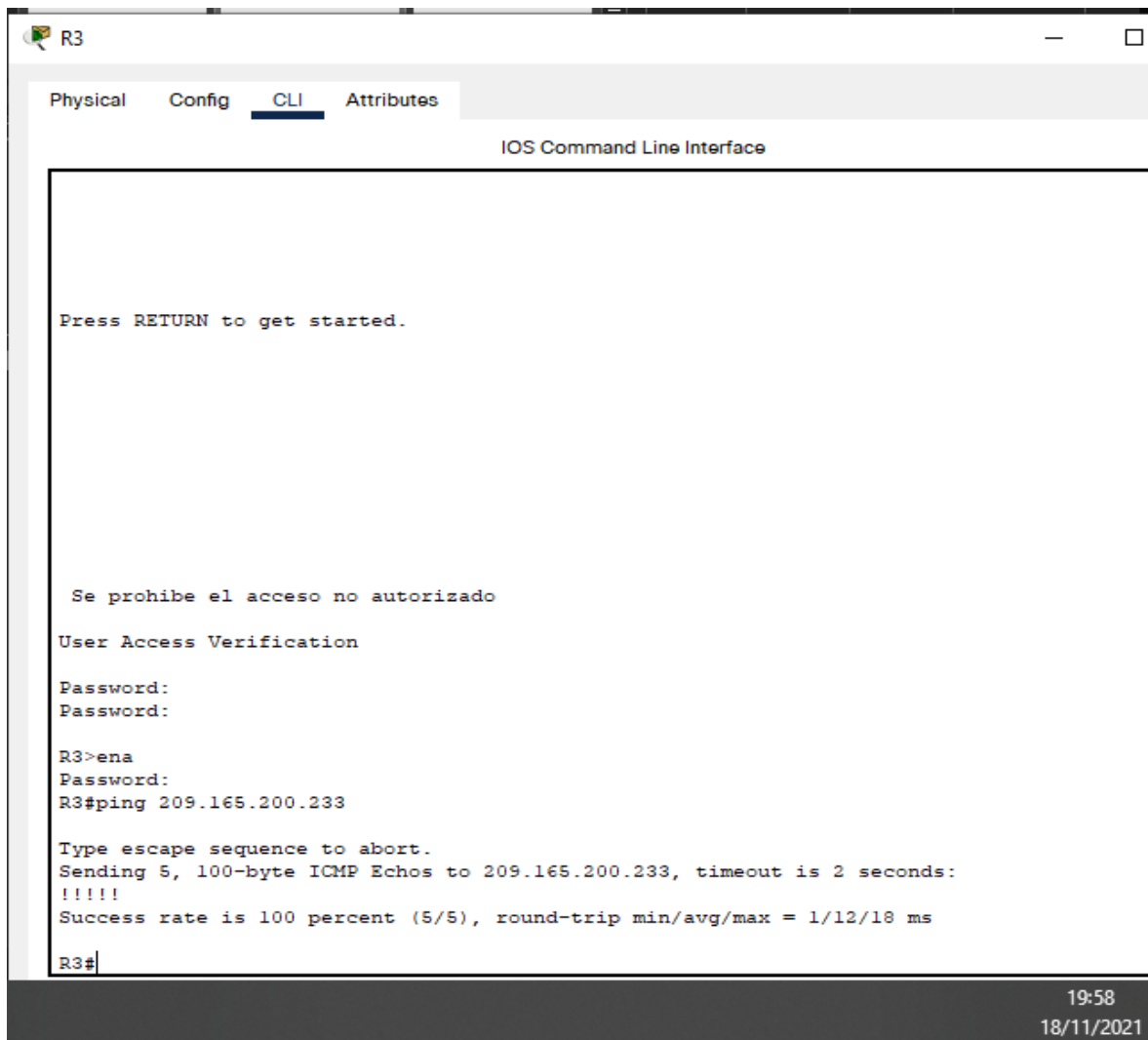
Fuente: Propia

Figura 13: Ping entre R2 y R3.



Fuente: Propia

Figura 14: Ping a servidor de internet



```
R3
Physical  Config  CLI  Attributes
IOS Command Line Interface

Press RETURN to get started.

Se prohíbe el acceso no autorizado

User Access Verification

Password:
Password:

R3>ena
Password:
R3#ping 209.165.200.233

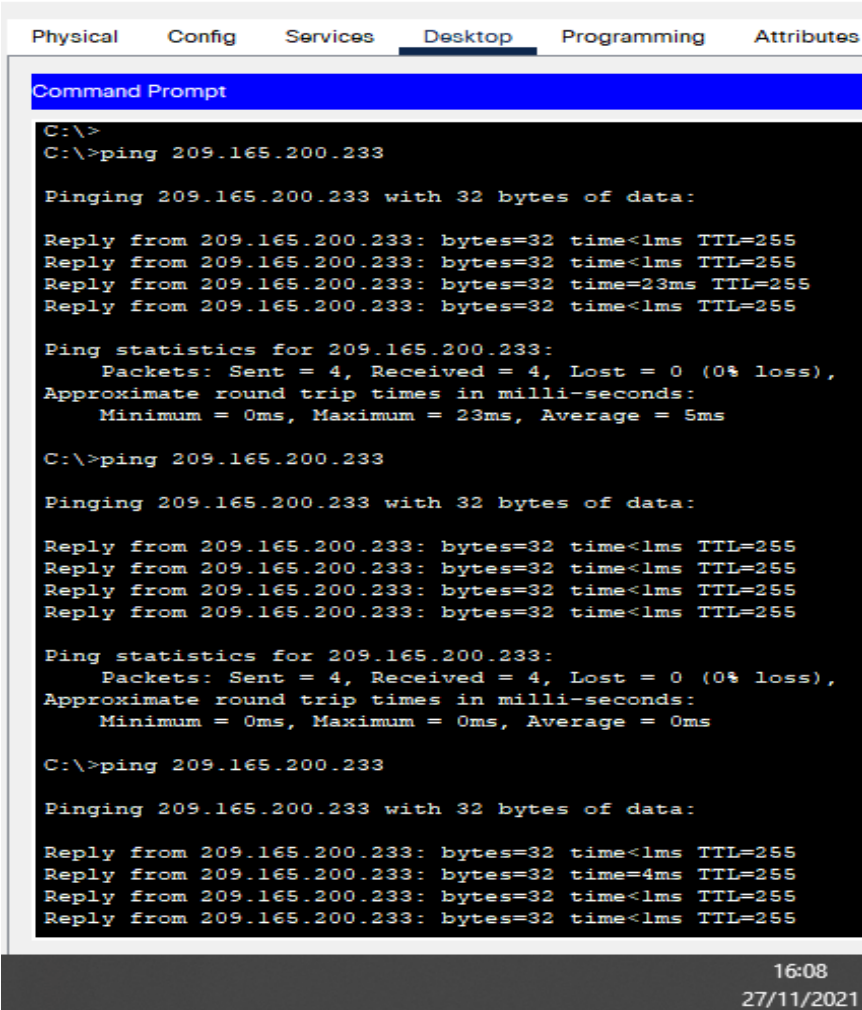
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.233, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/18 ms

R3#
```

19:58
18/11/2021

Fuente: Propia

Figura 15: Ping desde server a Ip .233P



Servidor de internet WEB

Physical Config Services Desktop Programming Attributes

Command Prompt

```
C:\>
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time=23ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 23ms, Average = 5ms

C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time=4ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
```

16:08
27/11/2021

Fuente: Propia

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14: Configuración del S1 y VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#exit</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#interface vlan 99 S1(config-if)# S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)# S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre>
Forzar el enlace troncal en la interfaz F0/5	<pre>S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config)#interface range fa0/6 S1(config-if-range)#switchport access</pre>

	vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Fuente: Propia

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15: Configuración de S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>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</pre>
Asignar la dirección IP de administración	<pre>S3(config)#interface vlan 99 S3(config-if)# S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit</pre>
Asignar el gateway predeterminado.	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfazF0/3	<pre>S3(config)#interface fastEthernet 0/3 S3(config-if)# S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit</pre>
Configurar el resto de los puertos comopuertos de acceso	<pre>S3(config)#interface range fa0/1- 2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit</pre>
Asignar F0/18 a la VLAN 21	<pre>S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit</pre>
Apagar todos los puertos sin usar	<pre>S3(config)#interface range fa0/1- 2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit</pre>

Fuente: Propia

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16: Configuración de R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 enG0/0/1	<pre> R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit </pre>
Configurar la subinterfaz 802.1Q .23 enG0/0/1	<pre> R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description accounting LAN de Ingenieria R1(config-subif)#enca </pre>

	<pre> psulation dot1q 23 R1(config- subif)#ip address 192.168.23. 1 255.255.25 5.0 R1(config-subif)#exit </pre>
<p>Configurar la subinterfaz 802.1Q .99 enG0/0/1</p>	<pre> R1(config)#interf ace gigabitEthernet 0/1.99 R1(config- subif)#descriptio n accounting LAN de Administracion R1(config- subif)#encapsula tion dot1q 99 R1(config- subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit </pre>
<p>Activar la interfaz G0/0/1</p>	<pre> R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown R1(config-if)#exit </pre>

Fuente: Propia

Paso 4: 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:

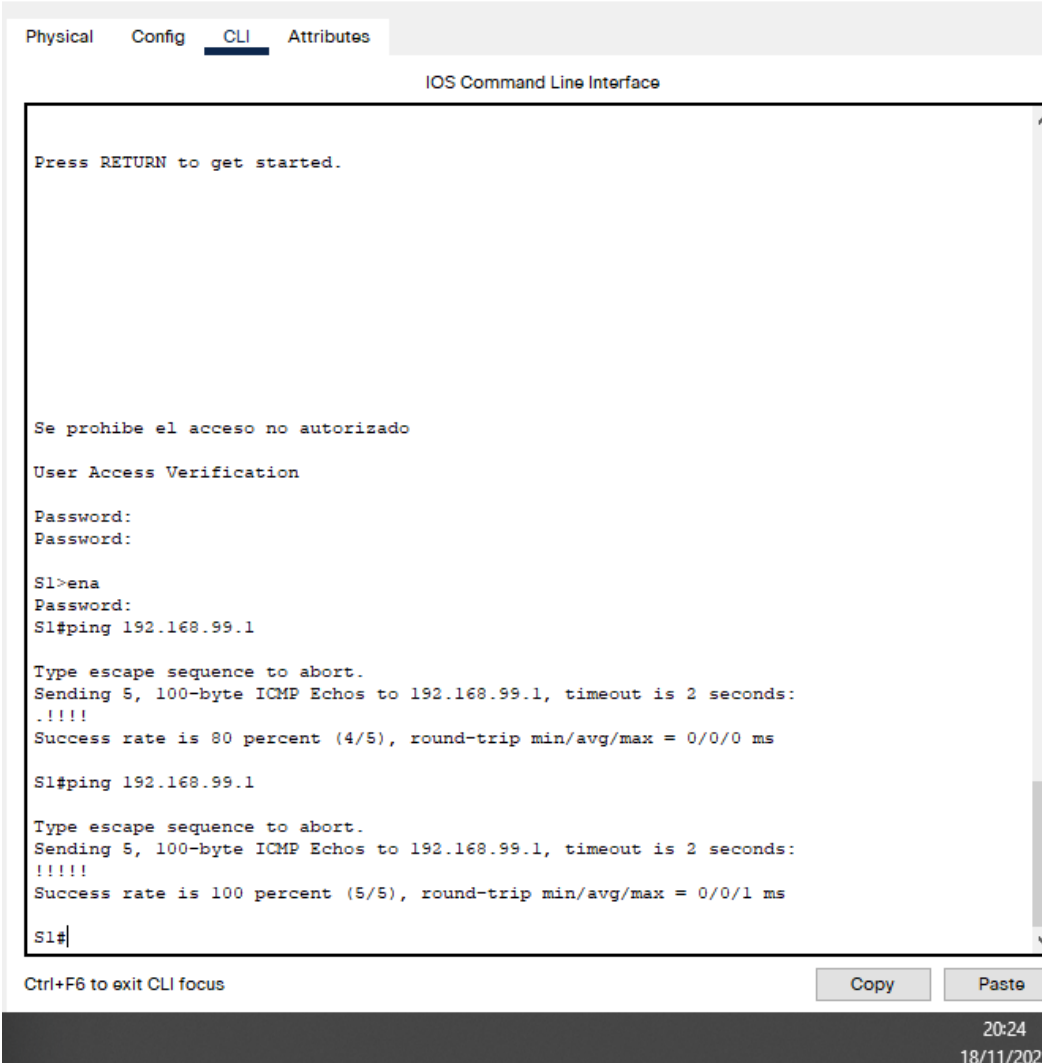
Tabla 17: Verificación de conectividad

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

	VLAN 21		192.168.21.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms S1#
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms S3#

Fuente: Propia

Figura 16: Ping desde S1 a R1 VLAN 99



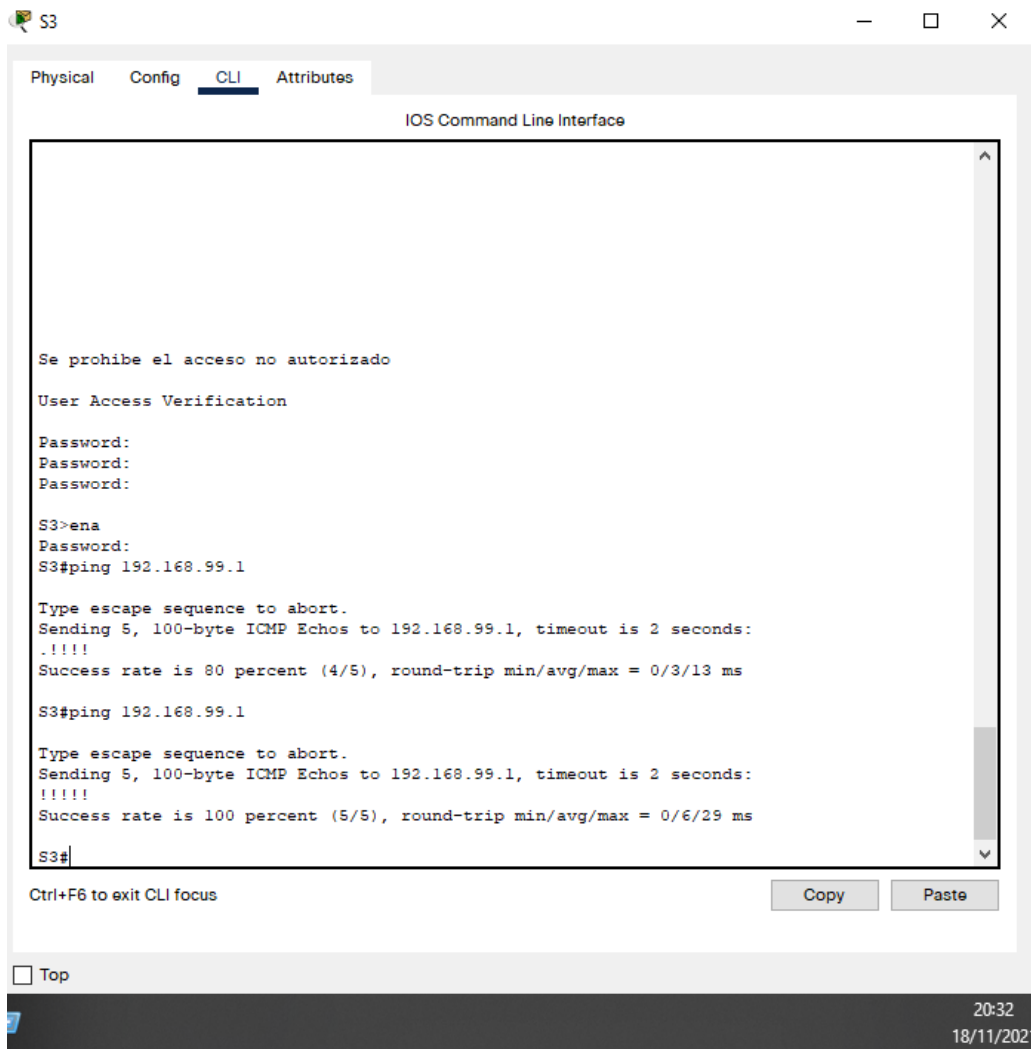
The screenshot shows the CLI interface of a network device (S1). The interface has tabs for Physical, Config, CLI (selected), and Attributes. The title bar reads "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
Press RETURN to get started.  
  
Se prohíbe el acceso no autorizado  
User Access Verification  
Password:  
Password:  
  
S1>ena  
Password:  
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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms  
  
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 = 0/0/1 ms  
  
S1#
```

At the bottom of the terminal window, there is a status bar with "Ctrl+F6 to exit CLI focus" on the left, "Copy" and "Paste" buttons in the center, and the time "20:24" and date "18/11/202" on the right.

Fuente: Propia

Figura 17: Ping desde S3 a R1 VLAN 99



Fuente: Propia

Figura 18: Ping desde S3 a R1 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 = 0/0/0 ms

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

S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

20:32
18/11/2021

Fuente: Propia

Figura 19: Ping desde S1 a R1 Vlan 21

```
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 = 0/0/3 ms

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#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

20:29
18/11/2021

Fuente: Propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18: Configuración de OSPF en el R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gi0/0/1.21 R1(config-router)#passive-interface gi0/0/1.23 R1(config-router)#passive-interface gi0/0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Fuente: Propia

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19: Configuración de OSPF en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo0

Desactive la sumarización automática.	R2(config-router)#no auto-summary
---------------------------------------	-----------------------------------

Fuente: Propia

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20: Configuración de OSPFv3 en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: Propia

Paso 4: 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: Verificación de información en 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	Show ip protocols

router?	
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf database

Fuente: Propia

Figura 20: comando Show ip protocols

```

[OK]
R1(config-router)#
20:13:09: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/2/0 from LOADING to FULL, Loading Done

R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0/1.21
    GigabitEthernet0/0/1.23
    GigabitEthernet0/0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:03:52
    192.168.6.1      110          00:03:11
    192.168.99.1     110          00:06:24
  Distance: (default is 110)

R1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

20:49
18/11/2021

Fuente: Propia

Figura 21: Comando para mostrar solo las rutas OSPF

```

R1# show ip route ospf
 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.2.0 [110/1626] via 172.16.1.2, 00:06:30, Serial0/2/0
 192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/1627] via 172.16.1.2, 00:05:12, Serial0/2/0
 192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/1627] via 172.16.1.2, 00:05:02, Serial0/2/0
 192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/1627] via 172.16.1.2, 00:04:52, Serial0/2/0
 209.165.200.0/29 is subnetted, 1 subnets
O   209.165.200.232 [110/74] via 172.16.1.2, 00:06:30, Serial0/2/0
R1#
  
```

Ctrl+F6 to exit CLI focus Copy Pas

20:51
18/11/2021

Fuente: Propia

Figura 22: Comando para mostrar la sección de OSPF

```

R1# show ip ospf database
      OSPF Router with ID (192.168.99.1) (Process ID 1)

      Router Link States (Area 0)

Link ID        ADV Router    Age         Seq#          Checksum Link count
192.168.99.1   192.168.99.1  536        0x80000005   0x00b2d3  5
10.10.10.10    10.10.10.10   384        0x80000008   0x00439c  5
192.168.6.1    192.168.6.1   343        0x80000005   0x00c5f6  5
R1#
  
```

Ctrl+F6 to exit CLI focus Copy P

20:52
18/11/2021

Fuente: Propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22: Configuración del R1 servidor de DHCP para VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30

Crear un pool de DHCP para la VLAN 21.	<pre> R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit </pre>
Crear un pool de DHCP para la VLAN 23	<pre> R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit </pre>

Fuente: Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23: Configuración de NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	<pre> R2(config)#user webuser privilege 15 secret cisco123 45 </pre>
Habilitar el servicio del servidor HTTP	No lo soporta

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No lo soporta
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gi0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248 Nombre del conjunto: INTERNET Validar El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

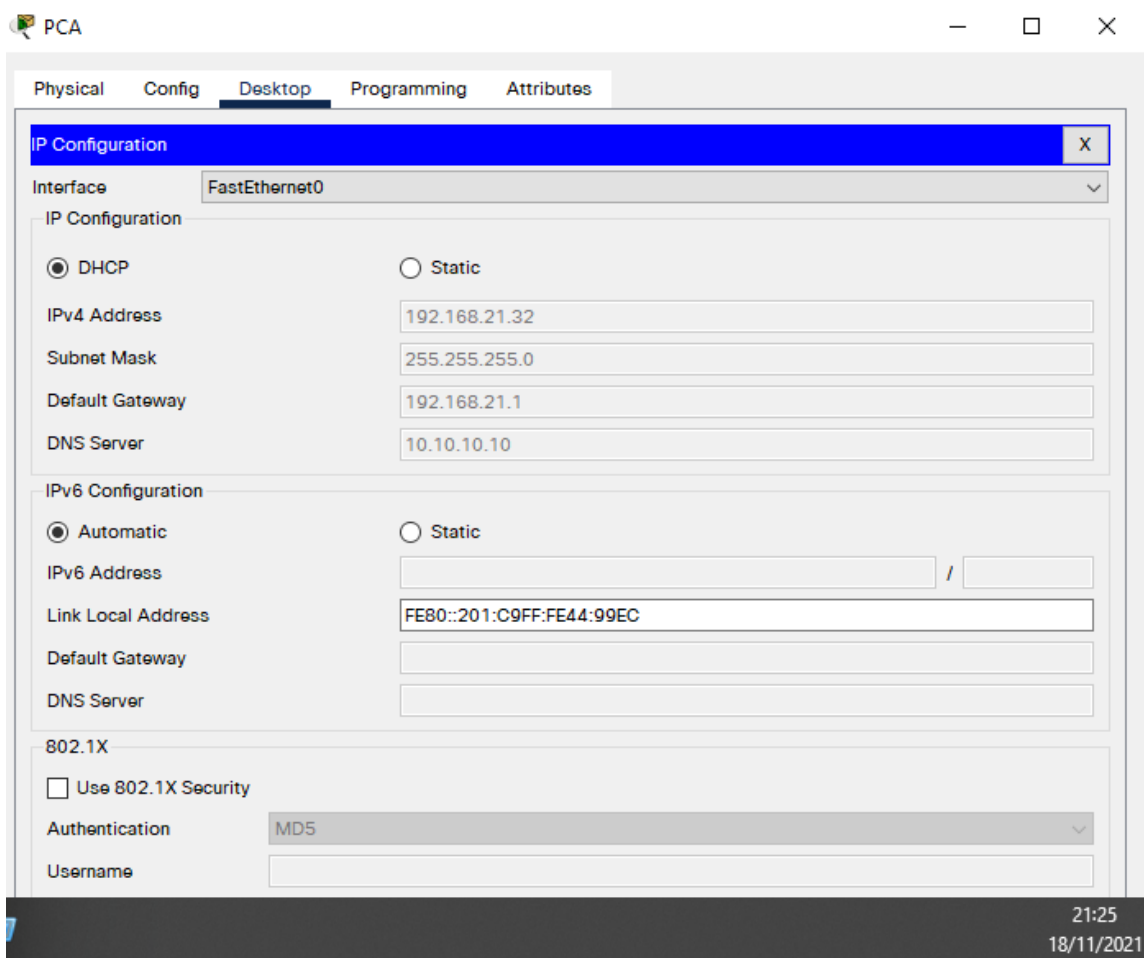
Fuente: Propia

Paso 3: 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.

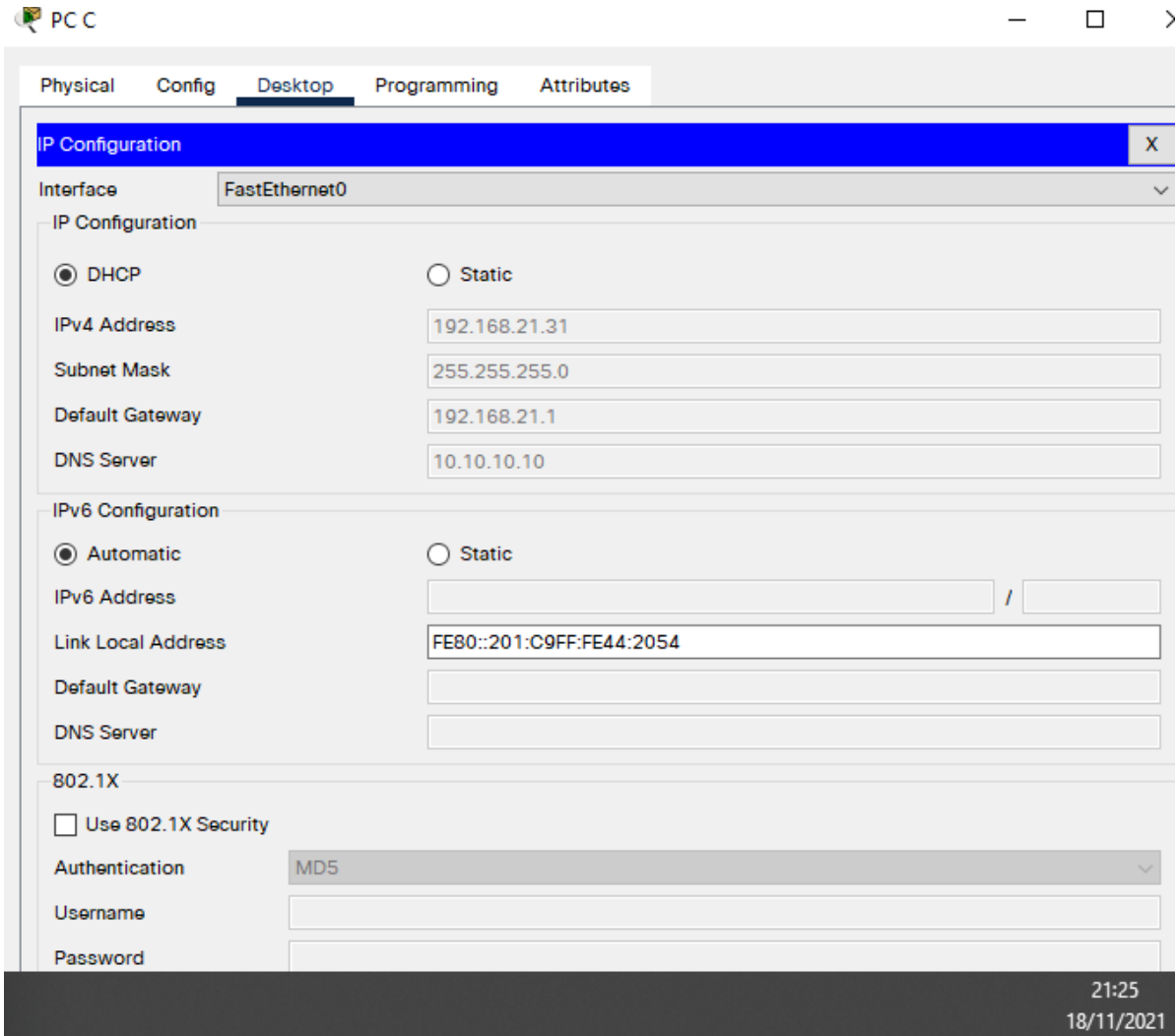
Pruebas y resultados:

Figura 23: Verificar PC-A adquiere información IP del servidor DHCP



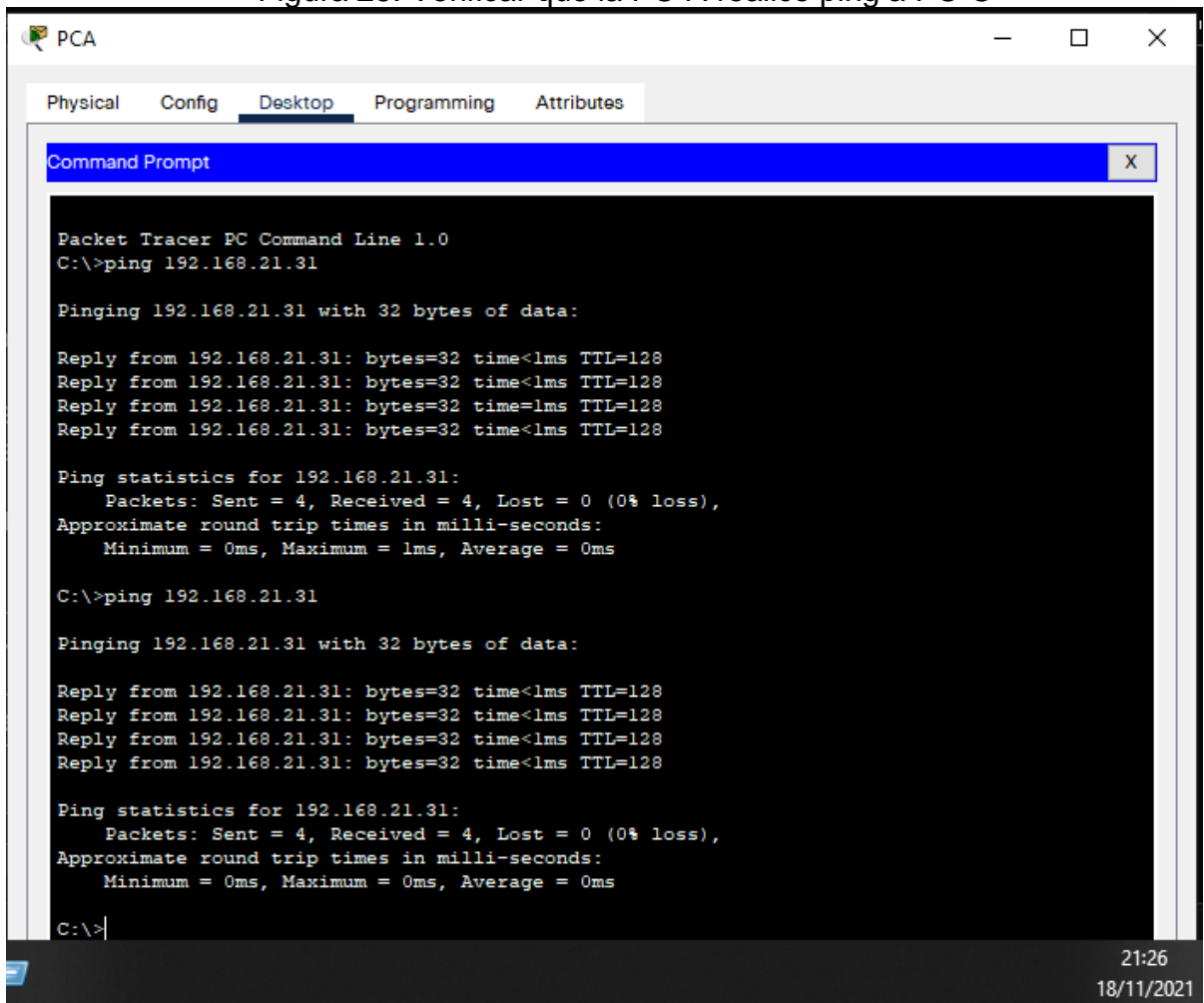
Fuente: Propia

Figura 24: Verificar PC-C adquiere información IP servidor DHCP



Fuente: Propia

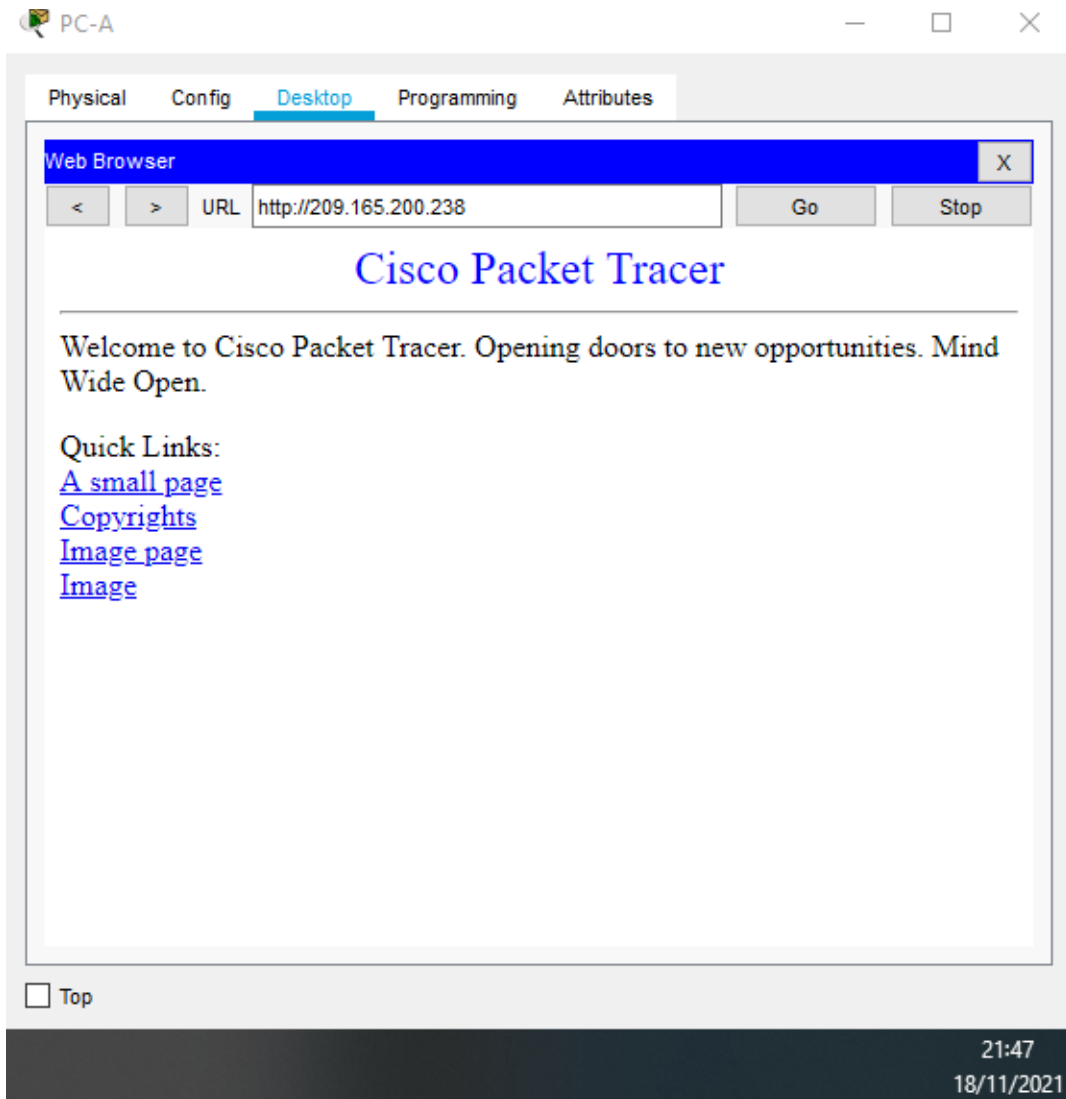
Figura 25: Verificar que la PC-A realice ping a PC-C



Fuente: Propia

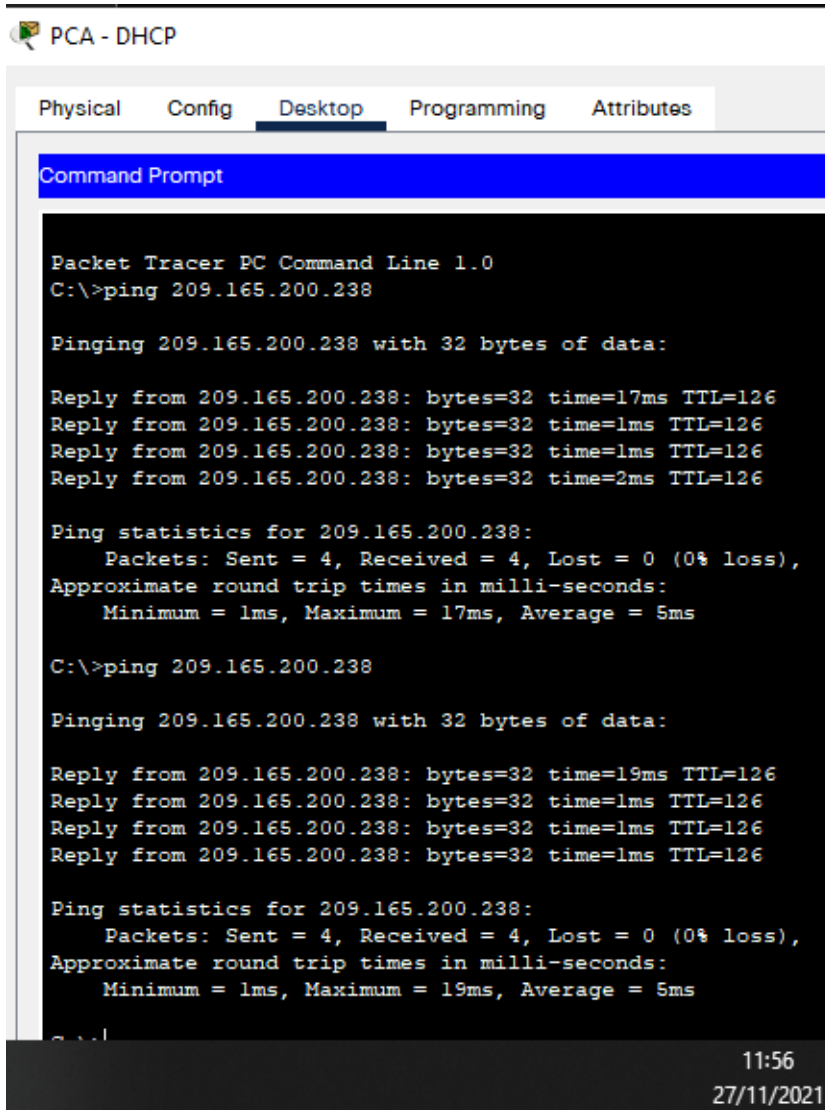
Nota: Quizá sea necesario deshabilitar el firewall de la PC.

Figura 26: Conectividad desde el PC-A hacia el servidor WEB



Fuente: Propia

Figura 27: Conectividad PC-A hacia servidor WEB – Prueba de Ping.



The screenshot shows a Packet Tracer interface for PC-A (DHCP) with the 'Desktop' tab selected. A Command Prompt window is open, displaying the results of two ping commands to the IP address 209.165.200.238. The first ping shows successful results with 0% loss and an average round trip time of 5ms. The second ping also shows successful results with 0% loss and an average round trip time of 5ms. The interface includes tabs for Physical, Config, Desktop, Programming, and Attributes. The Command Prompt title bar is blue and reads 'Command Prompt'. The background of the Command Prompt is black with white text. The bottom right corner of the Command Prompt shows the time '11:56' and the date '27/11/2021'.

```
Packet Tracer PC Command Line 1.0
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=17ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 5ms

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=19ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126
Reply from 209.165.200.238: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 5ms

C:\>
```

Fuente: Propia

Parte 6: Configurar NTP

Tabla 23: Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:00:00 05 Mar 2016 5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	

Fuente: Propia

Figura 28: Verificación de NTP en R1

```
poll interval is 4, last update was 10 sec ago.  
R1#show ntp status  
Clock is synchronized, stratum 6, reference is 172.16.1.2  
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24  
reference time is DA60355F.000000D5 (9:3:27.213 UTC Sat Mar 5 2016)  
clock offset is -1.00 msec, root delay is 4.00 msec  
root dispersion is 10.27 msec, peer dispersion is 0.12 msec.  
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system  
poll interval is 4, last update was 10 sec ago.  
R1#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

21:54

18/11/2021

Fuente: Propia

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

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

Tabla 24: Restringir acceso líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1establezca 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 172.16.1.1 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit

Fuente: Propia

Figura 29: Verificar funcionamiento de ACL

```

R2
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

poll interval is 5, last update was 20 sec ago.
R2#
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
R2(config)#do w
Building configuration...
[OK]
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#telnet 172.16.1.21
Trying 172.16.1.21 ...
% Connection timed out; remote host not responding
R2#telnet 172.16.1.23
Trying 172.16.1.23 ...
% Connection timed out; remote host not responding
R2#telnet 172.16.1.1
Trying 172.16.1.1 ...OpenSe prohíbe el acceso no autorizado

User Access Verification

Password:
Password:
Password:

[Connection to 172.16.1.1 closed by foreign host]
R2#
    
```

Fuente: Propia

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

Tabla 25: Descripción de comandos

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1(config)#show access-list
Restablecer los contadores de una lista de acceso	R1(config)#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1 (config)#interface Fa0/1 R1 (config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	R1 (config)#show ip nat translations Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1(config)#clear ip nat translation

Fuente: Propia

CONCLUSIONES

Se realiza las simulaciones a través de laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN, que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento

Se logra desarrollar la técnica de IP estática y dinámica para la configuración de los equipos, Switch, Router, PC's. y servidores a través de protocolos OSPF, NAT , Route, ETC.

Se comprendió como mediante el sistema Network Address Translation con su sigla NAT, podemos enviar paquetes entre dos redes que tienen direcciones IP incompatibles.

La herramienta virtual Packet tracer es de suma importancia para este tipo de proyectos, porque con la utilización y puesta en marcha de toda la estructura este programa podemos ver cómo funciona y como se programa este tipo de redes, facilitando tanto en diseño como en recursos económicos ya que no se tiene que empezar a realizar la red sin tener datos virtuales.

BIBLIOGRAFIA

- [1] GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, 12(1), 86-93.
- [2] GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, 14(1), 127-138.
- [3] BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.
- [4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, 16(1), 75-84.
- [5] BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.
- [6] BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovación y Tendencias en Ingeniería (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 Ingeniería (CONIITI)* (pp. 1-6). IEEE

- [8] Ali, A. N. A. (2012). Comparison study between IPV4 & IPV6. *International Journal of Computer Science Issues (IJCSI)*, 9(3), 314.
- [9] Aucapeña Macias, C. C. (2015). Diseño y simulación de una red que implemente enrutamiento estático para el protocolo de internet versión 4 y 6.
- [10] Garimella, P., Sung, Y. W. E., Zhang, N., & Rao, S. (2007, August). Characterizing VLAN usage in an operational network. In *Proceedings of the 2007 SIGCOMM workshop on Internet network management* (pp. 305-306).
- [11] Nguyen, V. G., & Kim, Y. H. (2016). SDN-based enterprise and campus networks: a case of VLAN management. *Journal of Information Processing Systems*, 12(3), 511-524.
- [12] Ortiz Arias, L. J. (2011). Topología de Red. *Redes de Comunicación I*.
- [13] Vázquez Viejo, J. M. (2011). *Diseño y desarrollo de una aplicación para el estudio comparativo de topologías de red* (Bachelor's thesis).