

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

REINALDO CHACON

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

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA  
CISCO

REINALDO CHACON

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

DIRECTOR:  
RAUL BAREÑO GUTIERREZ

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del jurado

---

Firma del jurado

BARRANCABERMEJA, 30 de noviembre de 2021

## AGRADECIMIENTOS

Mis más sinceros agradecimientos a Dios, a mis padres y toda mi familia que me ayudaron a alcanzar este sueño

## CONTENIDO

|   |    |
|---|----|
| AGRADECIMIENTOS.....  | 4  |
| CONTENIDO .....   | 5  |
| Lista de tablas.....  | 7  |
| Lista de figuras.....   | 9  |
| Resumen .....   | 11 |
| Abstract.....   | 12 |
| Introducción .....  | 13 |
| desarrollo .....  | 14 |
| 1.    Escenario 1 .....   | 14 |
| 1.1.    Parte 1. Construya la Red .....                             | 14 |
| 1.2.    Parte 2: Desarrolle el esquema de direccionamiento IP ..... | 14 |
| 1.3.    Parte 3: Configure aspectos básicos.....                    | 16 |
| 2.    escenario 2 .....   | 23 |
| 2.1.    Parte 1: Inicializar dispositivos .....                     | 23 |

|      |   |    |
|------|---|----|
| 2.2. | Parte 2: Configurar los parámetros básicos de los dispositivos .....          | 24 |
| 2.3. | Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN | 33 |
| 2.4. | Parte 4: Configurar el protocolo de routing dinámico OSPF .....               | 38 |
| 2.5. | Parte 5: Implementar DHCP y NAT para IPv4 .....                               | 41 |
| 2.6. | Parte 6: Configurar NTP .....   | 47 |
| 2.7. | Parte 7: Configurar y verificar las listas de control de acceso (ACL)..       | 48 |
|      | Conclusiones .....  | 52 |
|      | Bibliografía.....   | 53 |

## LISTA DE TRABLAS

|  |    |
|--|----|
| Tabla 1. Tabla de direccionamiento .....                                       | 15 |
| Tabla 2. Direccionamiento para LAN 1 y LAN 2 .....                             | 15 |
| Tabla 3. Direccionamiento escenario 1 .....                                    | 15 |
| Tabla 4. tareas para el PC-B .....   | 16 |
| Tabla 5. Configuración para el PC-A .....                                      | 18 |
| Tabla 6. Configuración de red para el PC-A .....                               | 20 |
| Tabla 7. Configuración de red para el PC-B .....                               | 21 |
| Tabla 8. Inicialización y cargue de routers y switches .....                   | 23 |
| Tabla 9. Configuración para el computador de Internet .....                    | 24 |
| Tabla 10. Configuración para el R1 .....                                       | 24 |
| Tabla 11. configuración para el R2 .....                                       | 25 |
| Tabla 12. Configuración para el R3 .....                                       | 27 |
| Tabla 13. Configuración para el S1 .....                                       | 28 |
| Tabla 14. Verificación de conectividad.....                                    | 30 |
| Tabla 15. Configuración de la seguridad del switch, VLAN y routing entre VLANs | 33 |

|  |    |
|--|----|
| Tabla 16. Configuración para el S3.....                                      | 34 |
| Tabla 17. configuración para el R1 .....                                     | 35 |
| Tabla 18. Verificación de la conectividad .....                              | 36 |
| Tabla 19. Implementación de OSPF en R1 .....                                 | 38 |
| Tabla 20. Configuración de OSPF en el R2.....                                | 39 |
| Tabla 21. Configuración de OSPFv3 en el R2 .....                             | 39 |
| Tabla 22. información de la OSPF .....                                       | 40 |
| Tabla 23. Configuración del R1 como servidor de DHCP para VLAN 21 - 23 ..... | 41 |
| Tabla 24. Configuración de la NAT estática y dinámica.....                   | 42 |
| Tabla 25. Verificación del protocolo DHCP y la NAT estática .....            | 43 |
| Tabla 26. NTP .....  | 47 |
| Tabla 27. Restricción del acceso a las líneas VTY .....                      | 48 |
| Tabla 28. Sintaxis para información de la red .....                          | 49 |



## LISTA DE FIGURAS

|  |    |
|--|----|
| Figura 1. Topología escenario 1 .....                                | 14 |
| Figura 3. configuración para el PC-A.....                            | 21 |
| Figura 4. Configuración de red para el PC-B .....                    | 22 |
| Figura 5. Base de datos de VLAN.....                                 | 23 |
| Figura 6. Configuración para el S3 .....                             | 29 |
| Figura 7. Verificación de conectividad desde el R2 hasta el R3 ..... | 32 |
| Figura 8. Comando ping para el default gateway.....                  | 32 |
| Figura 9. Verificación de la conectividad.....                       | 38 |
| Figura 11. información de OSPF.....                                  | 40 |
| Figura 12. Configuración DHCP en el PCA .....                        | 45 |
| Figura 13. Configuración DHCP en el PCC .....                        | 46 |
| Figura 14. Comando ping entre los dos computadores .....             | 46 |
| Figura 15. Servidor WEB .....  | 47 |
| Figura 16. NTP en el R1 y el R2 .....                                | 48 |
| Figura 18. Acceso R2 desde el R1 .....                               | 49 |

Figura 19. show access-lists .....50

Figura 20. show run .....51

Figura 21. show ip nat translations .....51

## RESUMEN

Fueron necesarias herramientas de simulación y realizar la respectiva documentación para los dos escenarios. Cada uno de estos presenta una configuración distinta y para su implantación se requirió de un entorno virtual, que se encarga de simular los equipos como si fueran reales. En este trabajo se empleó la herramienta Cisco Packet Tracer versión 8.0.1.0064, esta herramienta hace posible la simulación de sistemas de redes las cuales pueden ser implementadas en la vida real lo que facilita la comprensión y aplicación de las redes de informática. En el primer escenario propuesto se llevó a cabo la configuración de los equipos que se muestran en la topología, así pues, se enturó con una configuración IPv4 para cada una de las redes LAN requeridas.

En la segunda parte, para la topología dispuesta se realizó la configuración de todos los equipos bajo una configuración IPv4 y también con IPv6 para este segundo escenario fue necesario considerar los protocolos de configuración tales como OSPF, DHCP y NTP entre otros.

Palabras Clave: cisco, ipv4, ipv6, simulación, lan.

## ABSTRACT

Simulation tools and the respective documentation were necessary for the two scenarios. Each of these has a different configuration and for its implementation a virtual environment was required, which is responsible for simulating the equipment as if it were real. In this work the Cisco Packet tracer tool version 8.0.1.0064 was used, this tool makes possible the simulation of network systems which can be implemented in real life which facilitates the compression and application of computer networks. In the first proposed scenario, the configuration of the equipment shown in the topology was carried out, therefore, it was clouded with an IPv4 configuration for each of the required LAN networks.

In the second part, for the topology arranged the configuration of all the computers was made under an IPv4 configuration and with IPv6 for this second scenario it was necessary to consider the configuration protocols such as OSPF, DHCP and NTP among others.

Keywords: cisco, ipv4, ipv6, simulation, lan.

## INTRODUCCIÓN

A medida que los sistemas de redes continúan evolucionando en complejidad, están surgiendo nuevos planes de estudio y herramientas educativas para facilitar la enseñanza y el aprendizaje sobre la tecnología de redes.

Herramientas como Cisco Packet Tracer complementa el equipo físico en el aula al permitir crear una red con un número casi ilimitado de dispositivos, lo que fomenta la práctica, el descubrimiento y la resolución de problemas. El entorno de aprendizaje basado en simulación ayuda a desarrollar habilidades del siglo XXI, como la toma de decisiones, el pensamiento creativo y crítico y la resolución de problemas, con todo lo anterior es posible llevar a cabo el uso en protocolos tales como OSPF, DHCP y NTP entre otros, además, de poder realizar enrutamientos IPv4 e IPv6 todo el conjunto logra la implementación de redes que son aplicables a la vida real.

A continuación, se expone lo desarrollado para los dos escenarios propuestos como ejercicio práctico, de igual manera se logra evidenciar la aplicación de los principales protocolos de enrutamiento a lo largo de todo este documento con la finalidad de mostrar el dominio que se ha logrado obtener a lo largo del programa académico

## DESARROLLO

### 1. ESCENARIO 1

#### 1.1. Parte 1. Construya la Red

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

Figura 1. Topología escenario 1



Fuente: elaboración propia

#### 1.2. 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.

Considerando el direccionamiento 192.168.72.0 se construye la tabla de direccionamiento en la tabla 1.

Tabla 1. Tabla de direccionamiento

| <b>Ítem</b>                       | <b>Requerimiento</b>  |
|-----------------------------------|---|
| Dirección de Red                  | 192.168.X.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                             |
| R1 G0/0/0                         | Primera dirección de host de la subred LAN2                             |
| S1 SVI                            | segunda dirección de host de la subred LAN1                             |
| PC-A                              | Última dirección de host de la subred LAN1                              |
| PC-B                              | Última dirección de host de la subred LAN2                              |

Fuente: elaboración propia

Tabla 2. Direccionamiento para LAN 1 y LAN 2

|      | <b>Dirección de red</b> | <b>Máscara</b>  | <b>Primer IP</b> | <b>Broadcast</b> |
|------|-------------------------|-----------------|------------------|------------------|
| LAN1 | 192.168.72.128          | 255.255.255.128 | 192.168.72.1     | 192.168.72.127   |
| LAN2 | 192.168.72.192          | 255.255.255.192 | 192.168.72.129   | 192.168.72.191   |

Fuente: elaboración propia

Tabla 3. Direccionamiento escenario 1

| <b>Ítem</b> | <b>Requerimiento</b> |
|-------------|----------------------|
| R1 G0/0/1   | 192.168.72.1         |
| R1 G0/0/0   | 192.168.72.129       |
| S1 SVI      | 192.168.72.2         |
| PC-A        | 192.168.72.126       |
| PC-B        | 192.168.72.190       |

Fuente: elaboración propia

### 1.3. Parte 3: Configure aspectos básicos

#### 1.3.1. Paso 1: configurar los ajustes básicos

Tabla 4. tareas para el PC-B

| <b>Tarea</b>   | <b>Especificación</b>   |
|--|---|
| Desactivar la búsqueda DNS   | Router(config)#no ip<br>Router(config)#no ip domain   |
| Nombre del router  | Router(config)#hostnameR1   |
| Nombre de dominio  | R1(config)#ip domain-name ccna-lab.com  |
| Contraseña cifrada para el modo EXEC privilegiado                                    | R1(config)#enable secret ciscoenpass  |
| Contraseña de acceso a la consola  | R1(config)#line console 0<br>R1(config-line)#password ciscoconpass<br>R1(config-line)#login<br>R1(config-line)#exit<br>R1(config)#security pass |
| Establecer la longitud mínima para las contraseñas                                   | R1(config)#security passwords min-length 10   |
| Crear un usuario administrativo en la base de datos locales                          | R1(config)#username admin password admin1pass   |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line VTY 0 4<br>R1(config-line)#password admin1pass<br>R1(config-line)#login local   |



|  |   |
|--|---|
| Configurar VTY solo aceptando SSH          | R1(config-line)#transport input SSH   |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption  |
| Configure un MOTD Banner                   | R1(config)#banner motd # Acceso no autorizado<br>Reinaldo #   |
| Configurar interfaz G0/0/0                 | R1(config)#int g0/0/0<br>R1(config-if)#ip address 192.168.72.129<br>255.255.255.192<br>R1(config-if)#description #interfaz de LAN2#<br>R1(config-if)#no shutdown<br>R1(config-if)#exit  |
| Configurar interfaz G0/0/1                 | R1(config)#interface g0/0/1<br>R1(config-if)#description #Interfaz de LAN1#<br>R1(config-if)#ip address 192.168.72.1 255.255.255.128<br>R1(config-if)#no shutdown<br>R1(config-if)#exit   |
| Generar una clave de cifrado RSA           | R1(config)#ip domain name ccna-lab.com<br>R1(config)#crypto key generate RSA<br>The name for the keys will be: R1.ccna-lab.com<br>Choose the size of the key modulus in the range of 360 to 2048 for your<br>General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.<br>How many bits in the modulus [512]: 1024<br>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]<br>R1(config)#exit |

|  |  |
|--|--|
|  | <pre>*Mar 1 0:14:12.875: %SSH-5-ENABLED: SSH 1.99 has been enabled R1# %SYS-5-CONFIG_I: Configured from console by console wr Building configuration... [OK]</pre> |
|--|--|

Fuente: elaboración propia

Tabla 5. Configuración para el PC-A

| <b>Tarea</b>   | <b>Especificación</b>  |
|--|--|
| Desactivar la búsqueda DNS.  | S1(config)#ip default-gateway 192.168.72.1   |
| Nombre del switch  | Switch(config)#hostnameS1  |
| Nombre de dominio  | S1(config)#ip domain-name ccna-lab.com   |
| Contraseña cifrada para el modo EXEC privilegiado                                    | S1(config)#enable secret ciscoenpass   |
| Contraseña de acceso a la consola  | S1(config)#line console 0<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#exit     |
| Crear un usuario administrativo en la base de datos local                            | S1(config-line)#exit<br>S1(config)#username admin password dmin1pass                           |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config)#line VTY 0 15<br>S1(config-line)#password admin1pass<br>S1(config-line)#login local |

|  |  |
|--|--|
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S1(config-line)#transport input SSH<br>S1(config-line)#exit  |
| Cifrar las contraseñas de texto no cifrado                               | S1(config)#service password-encryption   |
| Configurar un MOTD Banner  | S1(config)#banner motd # Acceso no autorizado<br>Reinaldo #  |
| Generar una clave de cifrado RSA   | S1(config)#crypto key generate Rsa<br>The name for the keys will be: S1.ccna-lab.com<br>Choose the size of the key modulus in the range of 360 to 2048 for your<br>General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.<br>How many bits in the modulus [512]: 1024<br>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] |
| Configurar la interfaz de administración (SVI)                           | S1(config)#int vlan1<br>*Mar 1 0:7:20.32: %SSH-5-ENABLED: SSH 1.99 has been enabled<br>S1(config-if)#ip address 192.168.72.2<br>255.255.255.128<br>S1(config-if)#no shutdown<br>S1(config-if)#<br>%LINK-5-CHANGED: Interface Vlan1, changed state to up<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up                                      |

|  |   |
|--|---|
|  | S1(config-if)#exit  |
| Configuración del gateway predeterminado | S1(config)#ip de<br>S1(config)#ip default-gateway 192.168.72.1<br>S1(config)#exit<br>S1#<br>%SYS-5-CONFIG_I: Configured from console by console |

Fuente: elaboración propia

### 1.3.2. 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 6. Configuración de red para el PC-A

|                        |                              |
|------------------------|------------------------------|
| Descripción            | El PC-A está conectado al R1 |
| Dirección física       | 00E0.F7D3.BB48               |
| Dirección IP           | 192.168.72.125               |
| Máscara de subred      | 255.255.255.128              |
| Gateway predeterminado | 192.168.72.1                 |

Fuente: elaboración propia

Figura 2. configuración para el PC-A

```

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix . . . : 
    Physical Address. . . . . : 00E0.F7D3.BB48
    Link-local IPv6 Address . . . . . : FE80::2E0:F7FF:FED3:BB48
    IPv6 Address. . . . . : ::
    IPv4 Address. . . . . : 192.168.72.125
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 
                                192.168.72.1
    DHCP Servers . . . . . : 0.0.0.0
    DHCPv6 IAID . . . . . : 0.0.0.0
    DHCPv6 Client DUID. . . . . : 00-01-00-01-A4-A8-7E-31-00-E0-F7-D3-BB-48
    DNS Servers . . . . . : 
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix . . . : 
    Physical Address. . . . . : 000C.CF51.A499
    Link-local IPv6 Address . . . . . : 
    IPv6 Address. . . . . : 
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 
                                0.0.0.0
    DHCP Servers . . . . . : 0.0.0.0
    DHCPv6 IAID . . . . . : 
    DHCPv6 Client DUID. . . . . : 00-01-00-01-A4-A8-7E-31-00-E0-F7-D3-BB-48
    DNS Servers . . . . . : 
                                0.0.0.0

C:\>
C:\>
    
```

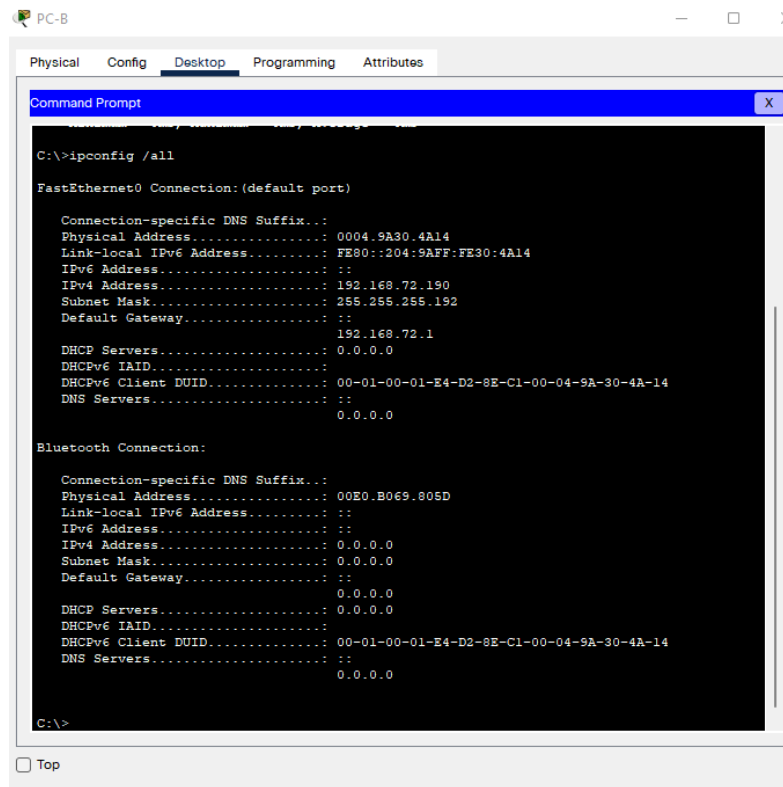
Fuente: elaboración propia

Tabla 7. Configuración de red para el PC-B

|                        |                              |
|------------------------|------------------------------|
| Descripción            | El PC-B está conectado al S1 |
| Dirección física       | 0004.9A30.4A14               |
| Dirección IP           | 192.168.72.190               |
| Máscara de subred      | 255.255.255.192              |
| Gateway predeterminado | 192.168.72.1                 |

Fuente: elaboración propia

Figura 3. Configuración de red para el PC-B



```
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 0004.9A30.4A14
    Link-local IPv6 Address . . . . . : FE80::204:9AFF:FE30:4A14
    IPv6 Address. . . . . : 
    IPv4 Address. . . . . : 192.168.72.190
    Subnet Mask. . . . . : 255.255.255.192
    Default Gateway. . . . . : 
    DHCP Servers. . . . . : 192.168.72.1
    DHCPv6 IAID. . . . . : 0.0.0.0
    DHCPv6 Client DUID. . . . . : 00-01-00-01-E4-D2-8E-C1-00-04-9A-30-4A-14
    DNS Servers. . . . . : 
    0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix... : 
    Physical Address. . . . . : 00E0.B069.805D
    Link-local IPv6 Address . . . . . : 
    IPv6 Address. . . . . : 
    IPv4 Address. . . . . : 0.0.0.0
    Subnet Mask. . . . . : 0.0.0.0
    Default Gateway. . . . . : 
    DHCP Servers. . . . . : 0.0.0.0
    DHCPv6 IAID. . . . . : 0.0.0.0
    DHCPv6 Client DUID. . . . . : 00-01-00-01-E4-D2-8E-C1-00-04-9A-30-4A-14
    DNS Servers. . . . . : 
    0.0.0.0

C:\>
```

Fuente: elaboración propia

## 2. ESECANARIO 2

### 2.1. Parte 1: Inicializar dispositivos

#### 2.1.1.1. 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 8. Inicialización y cargue de routers y switches

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

Fuente: elaboración propia

Figura 4. Base de datos de VLAN

```
Switch>show flash
Directory of flash:/

 1  -rw-   4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch>
```

Ctrl+F6 to exit CLI focus Coj

Fuente: elaboración propia

## 2.2. Parte 2: Configurar los parámetros básicos de los dispositivos

### 2.2.1. 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 9. Configuración para el computador de Internet

| <b>Elemento o tarea de configuración</b> | <b>Especificación</b> |
|--|-----------------------|
| 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   |
| Gateway predeterminado IPv6              | 2001:DB8:ACAD:2::1    |

Fuente: elaboración propia

### 2.2.2. Paso 2: Configurar R1

Tabla 10. Configuración para el R1

| <b>Elemento o tarea de configuración</b> | <b>Especificación</b>   |
|--|---|
| 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<br>R1(config)#line console 0                             |
| Contraseña de acceso a la consola        | R1(config-line)#password cisco<br>R1(config-line)#login<br>R1(config-line)#line vty 0 4 |



|  |   |
|--|---|
| Contraseña de acceso Telnnet               | R1(config-line)#password cisco<br>R1(config-line)#login<br>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 S0/0/0                            | R1(config)#ipv6 unicast-routing<br>R1(config)#int s0/0/0<br>R1(config-if)#ip address 172.16.1.1 255.255.255.252<br>R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no sh |
| Rutas predeterminadas                      | R1(config)#ip route 0.0.0.0 0.0.0.0 S0/0/0<br>R1(config)#ipv6 route ::/0 S0/0/0   |

Fuente: elaboración propia

### 2.2.3. Paso 3: Configurar R2

Tabla 11. configuración para el R2

| <b>Elemento o tarea de configuración</b> | <b>Especificación</b>                                       |
|--|---|
| Desactivar la búsqueda DNS               | Router(config)#no ip domain-lookup                          |
| Nombre del router                        | Router(config)#hostnameR2                                   |
| Contraseña de exec privilegiado cifrada  | R1(config)#enable secret class<br>R1(config)#line console 0 |
| Contraseña de acceso a la consola        | R1(config-line)#password cisco<br>R1(config-line)#login     |

|   |  |
|---|--|
|   | R1(config-line)#line vty 0 4   |
| Contraseña de acceso<br>Telnet                | R1(config-line)#password cisco<br>R1(config-line)#login<br>R1(config-line)#exit  |
| Cifrar las contraseñas de<br>texto no cifrado | R1(config)#service password-encryption   |
| Mensaje MOTD                                  | R1(config)#banner motd #se prohíbe el acceso no<br>autorizado Reinaldo#  |
| Interfaz S0/0/0                               | R2(config)#ipv6 unicast-routing<br>R2(config)#int s0/0/0<br>R2(config-if)#ip add<br>R2(config-if)#ip address 172.16.1.2 255.255.255.252<br>R2(config-if)#ipv6 add<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64<br>R2(config-if)#description conexión entre R3 - R1<br>R2(config-if)#no sh |
| Interfaz S0/0/1                               | R2(config)#int s0/0/1<br>R2(config-if)#ip address 172.16.2.1 255.255.255.252<br>R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64<br>R2(config-if)#clock rate 128000<br>R2(config-if)#no sh   |
| Interfaz G0/0 (simulación<br>de Internet)     | R2(config)#ipv6 unicast-routing<br>R2(config)#int G0/0<br>R2(config-if)#ip add<br>R2(config-if)#ip address 209.165.200.233<br>255.255.255.248<br>R2(config-if)#ipv6 add<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64<br>R2(config-if)#no sh   |

|  |   |
|--|---|
| Interfaz loopback 0<br>(servidor web simulado) | R2(config-if)#description servidor WEB<br>R2(config-if)#ip address 10.10.10.10<br>255.255.255.255 |
| Ruta predeterminada                            | R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0<br>R2(config)#ipv6 route ::/0 G0/0                       |

Fuente: elaboración propia

#### 2.2.4. Paso 4: Configurar R3

Tabla 12. Configuración para el R3

| <b>Elemento o tarea de configuración</b>   | <b>Especificación</b>   |
|--|---|
| Desactivar la búsqueda DNS                 | Router(config)#no ip domain-lookup  |
| Nombre del router                          | Router(config)#hostnameR3   |
| Contraseña de exec privilegiado cifrada    | R3(config)#enable secret class<br>R3(config)#line console 0                             |
| Contraseña de acceso a la consola          | R3(config-line)#password cisco<br>R3(config-line)#login<br>R3(config-line)#line vty 0 4 |
| Contraseña de acceso Telnet                | R3(config-line)#password cisco<br>R3(config-line)#login<br>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 Reinaldo#                  |
| Interfaz S0/0/1                            | R3(config)#int s0/0/1<br>R3(config-if)#ip address 172.16.2.2 255.255.255.252            |

|                       |   |
|-----------------------|---|
|                       | R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64<br>R3(config-if)#no sh                                   |
| Interfaz loopback 4   | R3(config)#int loopback 4<br>R3(config-if)#ip add 192.168.4.1 255.255.255.0<br>R3(config-if)#exit         |
| Interfaz loopback 5   | R3(config)#int loopback 5<br>R3(config-if)#ip add 192.168.5.1 255.255.255.0<br>R3(config-if)#exit         |
| Interfaz loopback 6   | R3(config)#int loopback 6<br>R3(config-if)#ip address 192.168.6.1 255.255.255.0<br>R3(config-if)#exit     |
| Interfaz loopback 7   | R3(config)#interface loopback 7<br>R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64<br>R3(config-if)#exit |
| Rutas predeterminadas | R3(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1<br>R3(config)#ipv6 route ::/0 S0/0/1                           |

Fuente: elaboración propia

## 2.2.5. Paso 5: Configurar S1

Tabla 13. Configuración para el S1

| <b>Elemento o tarea de configuración</b> | <b>Especificación</b>                                       |
|--|---|
| Desactivar la búsqueda DNS               | Switch(config)#no ip domain-lookup                          |
| Nombre del switch                        | Switch(config)#hostnameS1                                   |
| Contraseña de exec privilegiado cifrada  | S1(config)#enable secret class<br>S1(config)#line console 0 |
| Contraseña de acceso a la consola        | S1(config-line)#password cisco<br>S1(config-line)#login     |

|  |   |
|--|---|
|  | S1(config-line)#line vty 0 15   |
| Contraseña de acceso Telnet                | S1(config-line)#password cisco<br>S1(config-line)#login<br>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 Reinaldo #          |

Fuente: elaboración propia

### 2.2.6. Paso 6: Configurar el S3

Figura 5. Configuración para el S3

| <b>Elemento o tarea de configuración</b>   | <b>Especificación</b>  |
|--|--|
| 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<br>S3(config)#line console 0                              |
| Contraseña de acceso a la consola          | S3(config-line)#password cisco<br>S3(config-line)#login<br>S3(config-line)#line vty 0 15 |
| Contraseña de acceso Telnet                | S3(config-line)#password cisco<br>S3(config-line)#login<br>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 Reinaldo#                    |

Fuente: elaboración propia

### 2.2.7. 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 14. Verificación de conectividad

| Desde | A          | Dirección IP          | Resultados de ping   |
|-------|------------|-----------------------|--|
| R1    | R2, S0/0/0 | R1#ping<br>172.16.1.2 | Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:<br>!!!!<br>Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/13 ms |
| R2    | R3, S0/0/1 | R2#ping<br>172.16.2.2 | Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:<br>!!!!  |

|                |                        |                          |  |
|----------------|------------------------|--------------------------|--|
|                |                        |                          | Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms   |
| PC de Internet | Gateway predeterminado | C:\>ping 209.165.200.233 | <p>Pinging 209.165.200.233 with 32 bytes of data:</p> <p>Reply from 209.165.200.233: bytes=32 time&lt;1ms TTL=255</p> <p>Reply from 209.165.200.233: bytes=32 time=1ms TTL=255</p> <p>Reply from 209.165.200.233: bytes=32 time&lt;1ms TTL=255</p> <p>Reply from 209.165.200.233: bytes=32 time=1ms TTL=255</p> <p>Ping statistics for 209.165.200.233:</p> <p>    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</p> <p>    Approximate round trip times in milli-seconds:</p> <p>        Minimum = 0ms, Maximum = 1ms, Average = 0ms</p> |

Fuente: elaboración propia

Figura 6. Verificación de conectividad desde el R2 hasta el R3

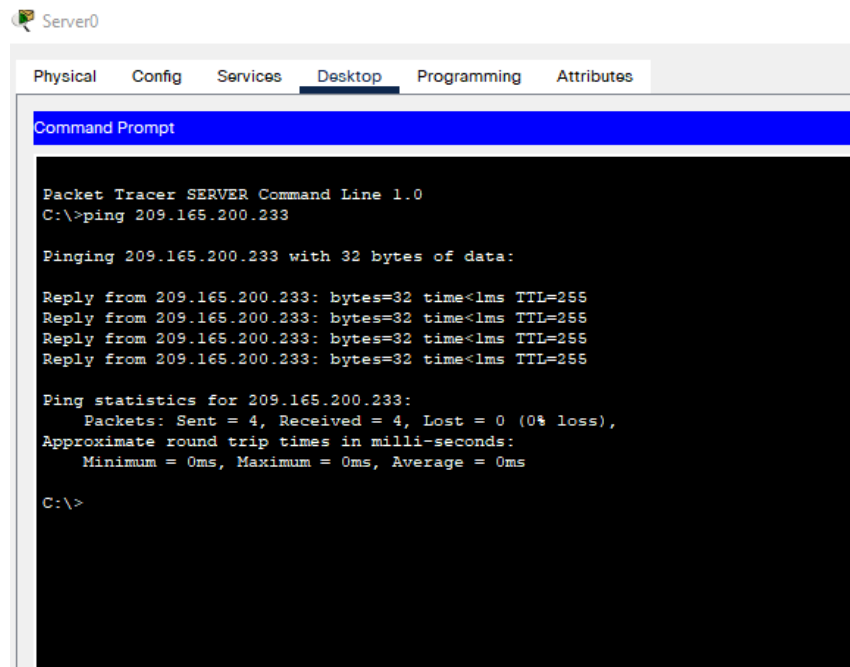
```
R2>en
Password:
R2#ping 172.16.2.2

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 = 2/5/12 ms

R2#
```

Fuente: elaboración propia

Figura 7. Comando ping para el default gateway



```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<lms TTL=255
Reply from 209.165.200.233: bytes=32 time<lms TTL=255
Reply from 209.165.200.233: bytes=32 time<lms TTL=255
Reply from 209.165.200.233: bytes=32 time<lms TTL=255

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

C:\>
```

Fuente: Elaboración propia



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

#### 2.3.1. Paso 1: Configurar S1

Tabla 15. Configuración de la seguridad del switch, VLAN y routing entre VLANs

| Elemento o tarea de configuración                         | Especificación  |
|---|---|
| Crear la base de datos de VLAN                            | Switch(config)#vlan 21<br>S1(config-vlan)#name contabilidad<br>S1(config-vlan)#vlan 23<br>S1(config-vlan)#name ingenieria<br>S1(config-vlan)#vlan 99<br>S1(config-vlan)#name administracion |
| Asignar la dirección IP de administración.                | S1(config)#int vlan 99<br>S1(config-if)#ip add 192.16.99.2 255.255.255.0<br>S1(config-if)#no sh<br>S1(config-if)#exit   |
| Asignar el gateway predeterminado                         | S1(config)#ip default-gateway 192.168.99.1  |
| Forzar el enlace troncal en la interfaz F0/3              | S1(config)#int f0/3<br>S1(config-if)#sw mode trunk  |
| Forzar el enlace troncal en la interfaz F0/5              | S1(config)#int f0/5<br>S1(config-if)#switchport trunk native vlan 1   |
| Configurar el resto de los puertos como puertos de acceso | S1(config)#int range f0/1- f0/2<br>S1(config-if-range)#sw mode access<br>S1(config-if-range)#int range f0/7- f0/24<br>S1(config-if-range)#sw mode access                                    |
| Asignar F0/6 a la VLAN 21                                 | S1(config-if)#int f0/6<br>S1(config-if)#sw mode access<br>S1(config-if)#sw access vlan 21   |

|                                   |   |
|-----------------------------------|---|
| Apagar todos los puertos sin usar | S1(config)#int range f0/7 - f0/24<br>S1(config-if-range)#sh |
|-----------------------------------|---|

Fuente: Elaboración propia

### 2.3.2. Paso 2: Configurar el S3

Tabla 16. Configuración para el S3

| Elemento o tarea de configuración                         | Especificación  |
|---|---|
| Crear la base de datos de VLAN                            | S3(config)#vlan 21<br>S3(config-vlan)#name contabilidad<br>S3(config-vlan)#vlan 23<br>S3(config-vlan)#name ingenieria<br>S3(config-vlan)#vlan 99<br>S3(config-vlan)#name administracion<br>S3(config-vlan)#exit<br>S3(config)#int vlan 99 |
| Asignar la dirección IP de administración                 | S3(config-if)#ip add 192.168.99.3<br>255.255.255.0<br>S3(config-if)#no sh   |
| Asignar el gateway predeterminado.                        | S3(config)#ip default-gateway<br>192.168.99.1   |
| Forzar el enlace troncal en la interfaz F0/3              | S3(config)#int f0/3<br>S3(config-if)#sw mode trunk<br>S3(config-if)#sw trunk native vlan 1<br>S3(config-if)#exit  |
| Configurar el resto de los puertos como puertos de acceso | S3(config)#int range f0/1 - f0/2<br>S3(config-if-range)#sw mode access<br>S3(config-if-range)#int ran f0/7 - f0/24  |

|                                   |  |
|-----------------------------------|--|
|                                   | S3(config-if-range)#sw mode access<br>S3(config-if-range)#exit |
| Asignar F0/18 a la VLAN 21        | S3(config)#int f0/18<br>S3(config-if)#sw acc vlan 21           |
| Apagar todos los puertos sin usar | S3(config-if)#int range f0/7 - f0/17<br>S3(config-if-range)#sh |

Fuente: elaboración propia

### 2.3.3. Paso 3: Configurar R1

Tabla 17. configuración para el R1

| <b>Elemento o tarea de configuración</b>     | <b>Especificación</b>   |
|--|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | R1(config)#int g0/1.21<br>R1(config-subif)#description Lan contabilidad<br>R1(config-subif)#enc dot1q 21<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0<br>R1(config-subif)#exit |
| Configurar la subinterfaz 802.1Q.23 en G0/1  | R1(config)#int g0/1.23<br>R1(config-subif)#desc Lan ingenieira<br>R1(config-subif)#en dot1q 23<br>R1(config-subif)#ip add 192.168.23.1 255.255.255.0<br>R1(config-subif)#exit               |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | R1(config)#int g0/1.99<br>R1(config-subif)#description LAn administracion<br>R1(config-subif)#en dot1q 99<br>R1(config-subif)#ip add 192.168.99.1 255.255.255.0<br>R1(config-subif)#exit    |

|                             |  |
|-----------------------------|--|
| Activar la interfaz<br>G0/1 | R1(config)#int g0/1<br>R1(config-if)#no sh |
|-----------------------------|--|

Fuente: elaboración propia

#### 2.3.4. 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 18. Verificación de la conectividad

| Desde | A                        | Dirección IP            | Resultados de ping  |
|-------|--------------------------|-------------------------|---|
| S1    | R1, dirección<br>VLAN 99 | S1#ping<br>192.168.99.1 | Type escape sequence to<br>abort.<br>Sending 5, 100-byte ICMP<br>Echos to 192.168.99.1, timeout<br>is 2 seconds:<br>!!!!<br>Success rate is 100 percent<br>(5/5), round-trip min/avg/max =<br>3/8/13 ms |
| S3    | R1, dirección<br>VLAN 99 | S3#ping<br>192.168.99.1 | Type escape sequence to<br>abort.   |

|    |                       |                      |  |
|----|-----------------------|----------------------|--|
|    |                       |                      | <p>Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:<br/> !!!!<br/> Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms</p>                                     |
| S1 | R1, dirección VLAN 21 | S1#ping 192.168.21.1 | <p>Type escape sequence to abort.<br/> Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:<br/> !!!!<br/> Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms</p> |
| S3 | R1, dirección VLAN 23 | S3#ping 192.168.23.1 | <p>Type escape sequence to abort.<br/> Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:<br/> !!!!<br/> Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms</p> |

Fuente: elaboración propia

Figura 8. Verificación de la conectividad

```

R1#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 = 0/3/8 ms
R1#

S1>en
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 = 0/0/1 ms
S1#

```

Fuente: elaboración propia

## 2.4. Parte 4: Configurar el protocolo de routing dinámico OSPF

### 2.4.1. Paso 1: Configurar OSPF en el R1

Tabla 19. Implementación de OSPF en R1

| Elemento o tarea de configuración                | Especificación   |
|--|--|
| Configurar OSPF área 0                           | R1(config)#router ospf 72  |
| Anunciar las redes conectadas directamente       | R1(config-router)#net 192.168.21.0 0.0.0.255 area 0<br>R1(config-router)#net 192.168.23.0 0.0.0.255 area 0<br>R1(config-router)#net 192.168.99.0 0.0.0.255 area 0<br>R1(config-router)#net 172.16.1.0 0.0.0.3 area 0 |
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface g0/1<br>R1(config-router)#passive-interface g0/1.21<br>R1(config-router)#passive-interface g0/1.23<br>R1(config-router)#passive-interface g0/1.99                                |
| Desactive la sumarización automática             | No es posible hacer para ospf  |

Fuente: elaboración propia

### 2.4.2. Paso 2: Configurar OSPF para el R2

Tabla 20. Configuración de OSPF en el R2

| <b>Elemento o tarea de configuración</b>          | <b>Especificación</b>   |
|---|---|
| Configurar OSPF área 0                            | R2(config)#router ospf 72   |
| Anunciar las redes conectadas directamente        | R2(config-router)#net 10.10.10.10 0.0.0.0 area 0<br>R2(config-router)#net 172.16.1.0 0.0.0.3 area 0<br>R2(config-router)#net 172.16.2.0 0.0.0.3 area 0<br>Nota: G0/0 fue omitido. |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface loopback 0  |
| Desactive la sumarización automática.             | No se puede hacer para este tipo de sistema de enrutamiento   |

Fuente: elaboración propia

### 2.4.3. Paso 3: Configurar OSPFv3 en el R2

Tabla 21. Configuración de OSPFv3 en el R2

| <b>Elemento o tarea de configuración</b> | <b>Especificación</b>  |
|--|--|
| Configurar OSPF área 0                   | R2(config)#int s0/0/0<br>R2(config-if)#ipv6 ospf 73 area 0<br>R2(config-if)#exit<br>R2(config)#int s0/0/1<br>R2(config-if)#ipv6 ospf 73 area 0<br>R2(config-if)#exit<br>R2(config)#int g0/0<br>R2(config-if)#ipv6 ospf 73 area 0 |

|   |  |
|---|--|
| Anunciar redes IPv4 conectadas directamente                         | No se puede hacer para las redes IPv4 conectadas directamente en esta red      |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | No se puede hacer en IPv6, la loopback no tiene direcciones bajo IPv6.         |
| Desactive la sumarización automática.                               | En este protocolo eso no se hace, se coloca la wildcard y en IPv6 no se puede. |

Fuente: elaboración propia

#### 2.4.4. 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 22. información de la OSPF

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

Fuente: elaboración propia

Figura 9. información de OSPF



```

R2#sh ip protocols
Routing Protocol is "ospf 72"
  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          00:12:01
    192.168.99.1     110          00:12:01
  Distance: (default is 110)

```

```

R2#show ip route ospf
O   192.168.21.0 [110/65] via 172.16.1.1, 00:12:31, Serial0/0/0
O   192.168.23.0 [110/65] via 172.16.1.1, 00:12:31, Serial0/0/0
O   192.168.99.0 [110/65] via 172.16.1.1, 00:12:31, Serial0/0/0
R2#

```

Fuente: elaboración propia

## 2.5. Parte 5: Implementar DHCP y NAT para IPv4

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

Tabla 23. Configuración del R1 como servidor de DHCP para VLAN 21 - 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<br>192.168.21.20  |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1<br>192.168.23.20  |
| Crear un pool de DHCP para la VLAN 21.   | R1(config)#ip dhcp pool ACCT<br>R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#default-router 192.168.21.1<br>R1(dhcp-config)#exit |

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

Fuente: elaboración propia

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

Tabla 24. Configuración de la NAT estática y dinámica

| <b>Elemento o tarea de configuración</b>   | <b>Especificación</b>  |
|--|--|
| Crear una base de datos local con una cuenta de usuario                                | R2(config)#username webuser privilege 15 password cisco12345   |
| Habilitar el servicio del servidor HTTP  | R2(config)#ip http server  |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | Esta acción no es posible  |
| Crear una NAT estática al servidor web.  | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237   |
| Asignar la interfaz interna y externa para la NAT estática                             | <pre>R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config-if)#int S0/0/0 R2(config-if)#ip nat inside</pre> |

|  |  |
|--|--|
|  | <pre>R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#int lo 0 R2(config-if)#ip nat inside</pre>   |
| Configurar la NAT dinámica dentro de una ACL privada   | <pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.7.255</pre> |
| Defina el pool de direcciones IP públicas utilizables. | <pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</pre>   |
| Definir la traducción de NAT dinámica                  | <pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>  |

Fuente: elaboración propia

### 2.5.3. 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.

Tabla 25. Verificación del protocolo DHCP y la NAT estática

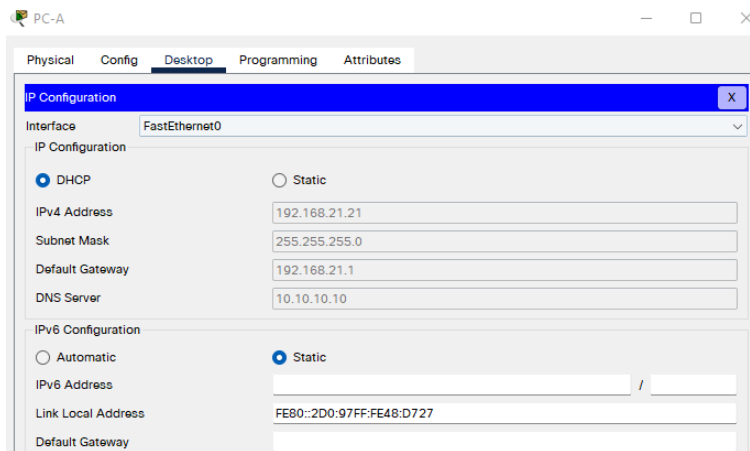
| Prueba  | Resultados  |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | <pre>C:\&gt;ping 192.168.21.22 Pinging 192.168.21.22 with 32 bytes of data: Reply from 192.168.21.22: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.21.22: bytes=32 time&lt;1ms TTL=128</pre> |

|  |  |
|--|--|
|  | <p>Reply from 192.168.21.22: bytes=32<br/>time&lt;1ms TTL=128</p> <p>Reply from 192.168.21.22: bytes=32<br/>time&lt;1ms TTL=128</p> <p>Ping statistics for 192.168.21.22:<br/>Packets: Sent = 4, Received = 4, Lost = 0<br/>(0% loss),<br/>Approximate round trip times in milli-seconds:<br/>Minimum = 0ms, Maximum = 0ms, Average<br/>= 0ms</p>  |
| <p>Verificar que la PC-C haya<br/>adquirido información de IP del<br/>servidor de DHCP</p>                                       | <p>Diríjase a las dos imágenes siguientes</p>  |
| <p>Verificar que la PC-A pueda<br/>hacer ping a la PC-C<br/>Nota: Quizá sea necesario<br/>deshabilitar el firewall de la PC.</p> | <p>Packet Tracer PC Command Line 1.0<br/>C:\&gt;ping 192.168.21.21<br/>Pinging 192.168.21.21 with 32 bytes of data:<br/>Reply from 192.168.21.21: bytes=32<br/>time&lt;1ms TTL=128<br/>Reply from 192.168.21.21: bytes=32<br/>time&lt;1ms TTL=128<br/>Reply from 192.168.21.21: bytes=32<br/>time&lt;1ms TTL=128<br/>Reply from 192.168.21.21: bytes=32<br/>time&lt;1ms TTL=128<br/>Ping statistics for 192.168.21.21:<br/>Packets: Sent = 4, Received = 4, Lost = 0<br/>(0% loss),<br/>Approximate round trip times in milli-seconds:</p> |

|   |   |
|---|---|
|   | Minimum = 0ms, Maximum = 0ms, Average = 0ms                           |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345 | Solo se puede con la siguiente dirección IP<br>http://209.165.200.238 |

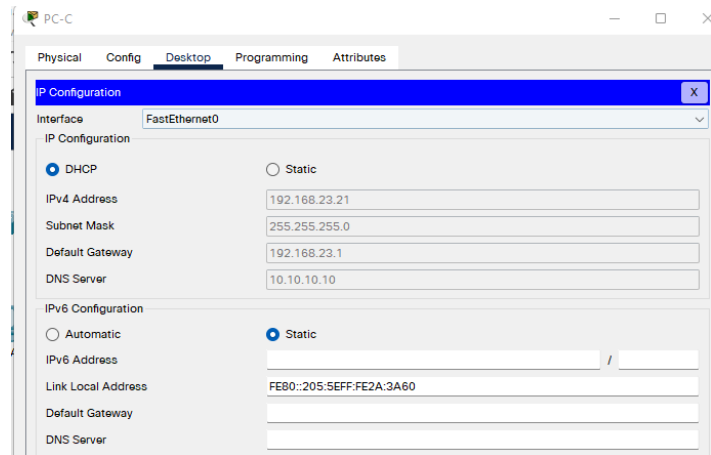
Fuente: elaboración propia

Figura 10. Configuración DHCP en el PCA



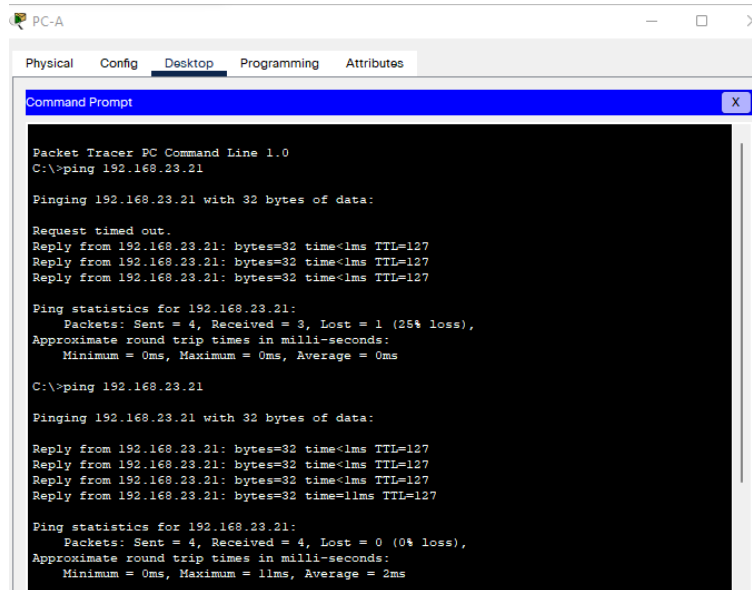
Fuente: elaboración propia

Figura 11. Configuración DHCP en el PCC



Fuente: elaboración propia

Figura 12. Comando ping entre los dos computadores



Fuente: elaboración propia

Figura 13. Servidor WEB



Fuente: elaboración propia

## 2.6. Parte 6: Configurar NTP

Tabla 26. NTP

| Elemento o tarea de configuración  | Especificación                                    |
|--|---|
| Ajuste la fecha y hora en R2.  | R2#clock set 09:00:00 05 march 2016               |
| Configure R2 como un maestro NTP.  | R2(config)#ntp master 5                           |
| Configurar R1 como un cliente NTP.                                       | R1(config)#ntp server 172.16.1.2                  |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1(config)#ntp update-calendar<br>R1(config)#exit |
| Verifique la configuración de NTP en R1.                                 | R1#sh clock                                       |

Fuente: elaboración propia

Figura 14. NTP en el R1 y el R2

The figure consists of two terminal windows side-by-side. The left window shows R2 in user mode, typing 'show clock' which returns the time '12:25:34.458 UTC Sat Mar 5 2016'. The right window shows R1 in user mode, typing 'en' to enter enable mode, then 'sh clock' which returns the time '12:26:22.766 UTC Sat Mar 5 2016'. Both windows have a footer that says 'Ctrl+F6 to exit CLI focus'.

Fuente: elaboración propia

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

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

Tabla 27. Restricción del acceso a las líneas VTY

| Elemento o tarea de configuración   | Especificación   |
|---|--|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | R1(config)#ip access-list standard ADMIN-MGT<br>R2(config-std-nacl)#permit host 172.16.1.1<br>R2(config-std-nacl)#deny any<br>R2(config-std-nacl)#exit |
| Aplicar la ACL con nombre a las líneas VTY  | R2(config)#line vty 0 4  |
| Permitir acceso por Telnet a las líneas de VTY  | R2(config-line)#ip access-class ADMIN-MGT in<br>R2(config-line)#transport input telnet   |
| Verificar que la ACL funcione como se espera  | R1#telnet 172.16.1.2   |

Fuente: elaboración propia



Figura 15. Acceso R2 desde el R1

```

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Opense prohíbe el acceso no autorizado Reinaldo

User Access Verification

Password:
R2>en
Password:
R2#exit

[Connection to 172.16.1.2 closed by foreign host]

```

Fuente: elaboración propia

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

Tabla 28. Sintaxis para información de la red

| Descripción del comando  | Entrada del estudiante (comando)   |
|--|--|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | R2#show access-lists<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255 (16 match(es))<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.0.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (4 match(es))<br>20 deny any |
| Restablecer los contadores de una lista de acceso  | R2#clear ip access-list counters   |
| ¿Qué comando se usa para mostrar qué ACL se aplica a   | R2#show run  |

|  |                                  |
|--|----------------------------------|
| una interfaz y la dirección en que se aplica?                            |                                  |
| ¿Con qué comando se muestran las traducciones NAT?                       | R2#show Access-lists             |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip access-list counters |

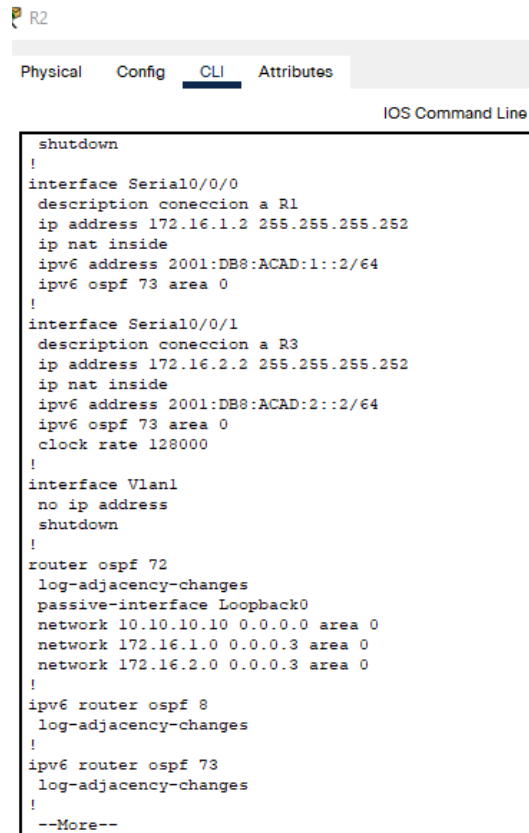
Fuente: elaboración propia

Figura 16. show access-lists

```
R2#show aCcess-lists
Standard IP access list 1
 10 permit 192.168.21.0 0.0.0.255 (16 match(es))
 20 permit 192.168.23.0 0.0.0.255
 30 permit 192.168.4.0 0.0.0.255
Standard IP access list ADMIN-MGT
 10 permit host 172.16.1.1 (4 match(es))
 20 deny any
```

Fuente: elaboración propia

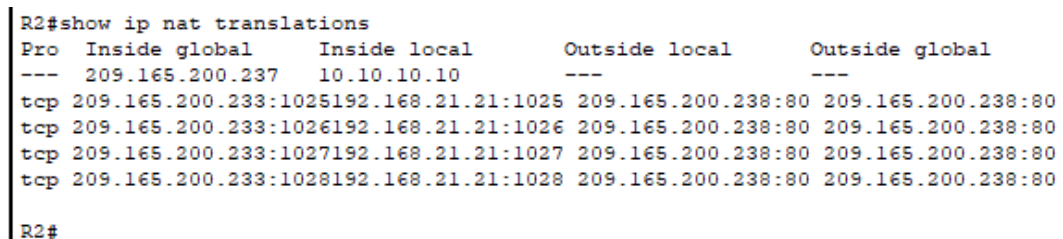
Figura 17. show run



```
shutdown
!
interface Serial10/0/0
description coneccion a R1
ip address 172.16.1.2 255.255.255.252
ip nat inside
ipv6 address 2001:DB8:ACAD:1::2/64
ipv6 ospf 73 area 0
!
interface Serial10/0/1
description coneccion a R3
ip address 172.16.2.2 255.255.255.252
ip nat inside
ipv6 address 2001:DB8:ACAD:2::2/64
ipv6 ospf 73 area 0
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 72
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
!
ipv6 router ospf 8
log-adjacency-changes
!
ipv6 router ospf 73
log-adjacency-changes
!
--More--
```

Fuente: elaboración propia

Figura 18. show ip nat translations



```
R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 ---
tcp 209.165.200.233:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1026192.168.21.21:1026 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1027192.168.21.21:1027 209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.233:1028192.168.21.21:1028 209.165.200.238:80 209.165.200.238:80
R2#
```

Fuente: elaboración propia

## CONCLUSIONES

Tras evaluar cada uno de los contenidos aquí empleados se infiere que los sistemas de redes continúan evolucionando en complejidad es por tanto que es necesario estar actualizado con la implementación de todos y cada uno de los protocolos que aquí se mencionan. Cada uno de estos permite hacer que los ordenadores se puedan comunicar de una manera eficiente, así como el enrutamiento que se realizó para cada uno de los dos escenarios propuestos, cuando se realiza una excelente implementación se tendrá como ventaja ahorro de tiempo a nivel empresarial y organizacional. Es claro que en todo el documento las implementaciones aquí realizadas cumplen a cabalidad con cada uno de los requerimientos ya que se puede evidenciar el correcto funcionamiento en cada uno de los dos escenarios propuestos.

## BIBLIOGRAFÍA

Al-Ani, D. R., & Al-Ani, A. R. (2018). The Performance of IPv4 and IPv6 in Terms of Routing Protocols using GNS 3 Simulator. *Procedia Computer Science*, 130, 1051–1056. doi:10.1016/j.procs.2018.04.147

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. (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). 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

Carpenter, M. (2003). The stock market and innovative capability in the New Economy: the optical networking industry. *Industrial and Corporate Change*, 12(5), 963–1034. doi:10.1093/icc/12.5.963

DiCerbo, K. E. (2009). Hands-On Instruction in the Cisco Networking Academy. 2009 Fifth International Conference on Networking and Services. doi:10.1109/icns.2009.23

Dennis, A., Cakir, H., Korkmaz, A., Duffy, T., Bichelmeyer, B., & Bunnage, J. (2006). Student Achievement in the Cisco Networking Academy: Performance in the CCNA1 Course. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). doi:10.1109/hicss.2006.442

Gutiérrez, 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.

Qiao, X., Wang, H., Tan, W., Vasilakos, A. V., Chen, J., & Blake, M. B. (2019). A survey of applications research on content-centric networking. China Communications, 16(9), 122–140. doi:10.23919/jcc.2019.09.009

Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. Computer Standards & Interfaces, 68, 103391. doi: 10.1016/j.csi.2019.103391

Moss, N., & Smith, A. (2010). Large Scale Delivery of Cisco Networking Academy Program by Blended Distance Learning. 2010 Sixth International Conference on Networking and Services. doi:10.1109/icns.2010.52

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.

Riley, C., Flannagan, M. E., Fuller, R., Khan, U., Lawson, W. A., O'Brien, K., & Walshaw, M. (2003). Cisco Technologies, Routers, and Switches. The Best Damn Cisco Internetworking Book Period, 1–89. doi:10.1016/b978-193183691-3/50018-3

Sarala, S., & Krishnamoorthi, K. (2020). Enhanced packet routing queuing model in optical burst switching network using queue-based dynamic optical route scheduling. *Microprocessors and Microsystems*, 79, 103296. doi: 10.1016/j.micpro.2020.103296

Tse, E. S. H. (2005). Switch fabric design for high performance IP routers: A survey. *Journal of Systems Architecture*, 51(10-11), 571–601. doi: 10.1016/j.sysarc.2004.12.005

Žarković, S. D., Shayesteh, E., & Hilber, P. (2021). Integrated reliability centered distribution system planning — Cable routing and switch placement. *Energy Reports*, 7, 3099–3115. doi: 10.1016/j.egy.2021.05.045