

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS MATEO CRUZ GIL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

INGENIERIA ELECTRONICA

PEREIRA – RISARALDA

AÑO 2021

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS MATEO CRUZ GIL

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) OPCIÓN DE GRADO PARA EL TÍTULO DE INGENIERÍA ELECTRONICA

HECTOR HERRERA

TUTOR ASESOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

INGENIERÍA ELECTRONICA

PEREIRA – RISARALDA

AÑO 2021

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Pereira, 16 de julio de 2021

## AGRADECIMIENTOS

Gracias al ejemplo de mi familia con sus principios y valores me han forjado como persona íntegra, entendiendo la importancia que tiene el estudio para mi vida personal y sociedad. También resalto la grandiosa labor y reto que tienen los docentes de transmitirnos su conocimientos y experiencias.

## CONTENIDO

GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCION .....	11
DESARROLLO DEL PROYECTO .....	12
ESCENARIO 1.....	12
ESCENARIO 2.....	32
CONCLUSIONES .....	59

## LISTA DE TABLAS

TABLA 1. VLAN .....	12
TABLA 2. ASIGNACIÓN DE DIRECCIONES .....	12
TABLA 3. TAREAS DE CONFIGURACIÓN EN R1 .....	14
TABLA 4. TAREAS DE CONFIGURACIÓN PARA EL SWITCH S1 Y S2.....	17
TABLA 5. TAREAS DE CONFIGURACIÓN VLAN Y TRONCALES PARA EL SWITCH S1 .....	19
TABLA 6. TAREAS DE CONFIGURACIÓN SWITCH S2.....	21
TABLA 7. CONFIGURACIÓN DE R1 DHCP.....	23
TABLA 8. NETWORK PC-A.....	24
TABLA 9. NETWORK PC-B.....	24
TABLA 10. CONFIGURACIÓN DE LA COMPUTADORA DE INTERNET.....	34
TABLA 11. VERIFICACIÓN DE LA CONECTIVIDAD DE LOS DISPOSITIVOS....	41
TABLA 12. CONECTIVIDAD DE LA RED.....	46
TABLA 13. VERIFICACIÓN DE LA INFORMACIÓN DE OSPF.....	50
TABLA 14. CONFIGURACIÓN NTP EN R2.....	56
TABLA 15. COMANDOS DE VERIFICACIÓN.....	58

## LISTA DE FIGURAS

FIGURA 1. TOPOLOGÍA ESCENARIO 1 .....	12
FIGURA 2. PING PC-A A R1, G0/1.2.....	26
FIGURA 3. PING DESDE PC-A A R1, G0/0/1.3 .....	26
FIGURA 4. PING DESDE PC-A A R1, G0/0/1.4 .....	27
FIGURA 5. PING DESDE PC-A AS1, VLAN 4.....	27
FIGURA 6. PING DESDE PC-A A S2, VLAN 4.....	28
FIGURA 7. PING DESDE PC-A A PC-B.....	28
FIGURA 8. PING DESDE PC-B A R1 BUCLE 0 .....	29
FIGURA 9. PING DESDE PC-B A R1, G0/0/1.2 .....	29
FIGURA 10. PING DESDE PC-B A R1, G0/0/1.3 .....	30
FIGURA 11. PING DESDE PC-B A R1, G0/0/1.4 .....	30
FIGURA 12. PING DESDE PC-B A S1, VLAN 4.....	31
FIGURA 13. PING DESDE PC-B A S2, VLAN 4.....	31
FIGURA 14. TOPOLOGÍA ESCENARIO 2 .....	32
FIGURA 15. COMANDOS DE PING DESDE S1 .....	48
FIGURA 16. COMANDOS DE PING DESDE S3.....	48
FIGURA 17. COMANDO DE “SHOW IP PROTOCOLS” EN R1 .....	51
FIGURA 18. COMANDO DE “SHOW IP ROUTE OSPF” EN R1 .....	51
FIGURA 19. COMANDO DE “SHOW IP OSPF DATABASE” EN R1 .....	52
FIGURA 20. CONFIGURACIÓN PC-A .....	54
FIGURA 21. CONFIGURACIÓN PC-C .....	55
FIGURA 22. PING DE PC-A A PC-C .....	55
FIGURA 23. NAVEGADOR WEB .....	56
FIGURA 24. CONFIGURACIÓN DE NTP EN R1 .....	56
FIGURA 25. FUNCIONAMIENTO DE LA ACL.....	57

## GLOSARIO

**ETHERNET:** Es la tecnología LAN más utilizada hoy en día. Ethernet funciona en la capa de enlace de datos y en la capa física. Es una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3.

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

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

**VLAN:** Virtual LAN (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch.

**SÍMBOLO DE SISTEMA:** Conocido como CMD.exe es un interprete de comandos de los sistemas operativos de Windows.



## RESUMEN

El presente trabajo están las actividades evaluativas que tiene el diplomado de profundización CCNA de la empresa de CISCO, donde demostramos los conocimientos adquiridos durante todo el proceso formativo que tiene. Este se divide en dos escenarios.

Se configuran un grupo de dispositivos que lo conforman switches, routers y PCs con el objetivo de conectarlos a través de IPv4 e IPv6, esta red es administrable y con niveles de seguridad, los enrutamientos son con VLAN y DHCP.

**PALABRAS CLAVES:** Dispositivos, CISCO, Seguridad, Conexión.

## ABSTRACT

The present work is one of the evaluative activities that the CISCO company CCNA deepening diploma has, where we demonstrate the knowledge acquired throughout the training process that it has. This is divided into two scenarios.

Scenario one, a group of devices is configured that is made up of two switches, a router and two PCs in order to connect them through IPv4 and IPv6, this network is manageable and with security levels, the routing is with VLAN and DHCP.

KEY WORDS: Devices, CISCO, Security, Connection.

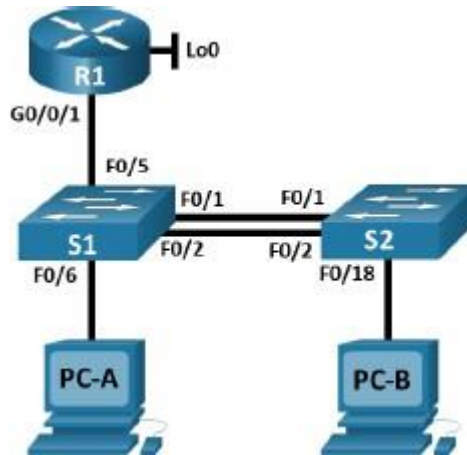
## INTRODUCCION

En este trabajo se encuentra el desarrollo paso a paso de las actividades que indica el primer escenario del diplomado, están las evidencias del uso del software Packet Tracer y se documentan los comandos que se utilizan para la configuración y prueba de los dispositivos de la red que se simula.

Culminando esta actividad se da a conocer las competencias y habilidades que generan las estrategias de aprendizaje que se implementaron para realizar cada una de las actividades de las que se compone este diplomado.

## DESARROLLO DEL PROYECTO ESCENARIO 1

Figura 1. Topología escenario 1



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. El router y el switch también deben administrarse de forma segura. Configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1. VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla 2. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
R1 G0/0/1.2	2001:db5:acad:a :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
R1 G0/0/1.3	2001:db5:acad:b :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
R1 G0/0/1.4	2001:db5:acad:c :1 /64	No corresponde

R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
VLAN S1 4	2001:db5:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
S2 VLAN 4	2001:db5:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db5:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db5:acad:b: :50 /64	fe80::1

## Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Comandos en R1:

```
Router>enable
Router#erase startup-config
Router#reload
```

Comandos en S1:

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
```

```

Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

```

## Comandos en S2:

```

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]

```

## Paso 2: Configurar R1

Tabla 3. Tareas de configuración en R1

<i>Tarea</i>	<i>Especificación</i>
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: <b>admin</b> Password: <b>admin1pass</b>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Habilitar el routing IPv6	

Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como <b>fe80: :1</b> Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como <b>fe80::1</b>
Generar una clave de cifrado RSA	Módulo de 1024 bits

### Comandos R1:

```

Router#configure terminal
Router(config)#no ip domain-lookup

Router(config)#hostname R1

R1(config)#ip domain-name ccna-lab.com

R1(config)#enable secret ciscoenpass

R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

R1(config)#security passwords min-length 10

R1(config)#username admin privilege 15 secret adminlpass

R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit

R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit

R1(config)#service password-encryption

```

```

R1(config)#banner motd "ACCESO NO AUTORIZADO"

R1(config)#ipv6 unicast-routing

R1(config)#interface gi0/1.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#description LAN to VLAN2
R1(config-subif)#ip add 10.21.5.1 255.255.255.192
R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip add 10.21.5.65 255.255.255.224
R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#description LAN to VLAN3
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface gi0/1.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#ip add 10.21.5.97 255.255.255.248
R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 add fe80::1 link-local
R1(config-subif)#description LAN to VLAN4
R1(config-subif)#no shutdown
R1(config-subif)#exit

R1(config)#interface gi0/1.6
R1(config-subif)#encapsulation dot1q 6
R1(config-subif)#exit
R1(config)#interface gi0/1
R1(config-if)#no shutdown

R1(config)#interface lo0
R1(config-if)#description LAN to Loopback0
R1(config-if)#ip add 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 add 2001:db5:acad:209::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#exit

R1(config)#crypto key generate rsa

```



Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Tareas de configuración para el Switch S1 Y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	<b>S1 o S2, según proceda</b>
Nombre de dominio	<b>ccna-lab.com</b>
Contraseña cifrada para el modo EXEC privilegiado	<b>ciscoenpass</b>
Contraseña de acceso a la consola	<b>ciscoconpass</b>
Crear un usuario administrativo en la base de datos local	Nombre de usuario: <b>admin</b> Password: <b>admin1pass</b>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	<b>Módulo de 1024 bits</b>
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como <b>FE80: :98 para S1 y FE80: :99 para S2</b> Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4

Comandos para configurar S1:

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
```

```
S1(config)#ip domain-name ccna-lab.com
```

```

S1(config)#enable secret ciscoenpass

S1(config)#line con 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit

S1(config)#username admin privilege 15 secret adminlpass

S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit

S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit

S1(config)#service password-encryption

S1(config)# banner motd "ACCESO NO AUTORIZADO"

S1(config)#crypto key generate rsa

S1(config)#interface vlan 4
S1(config-if)#ip add 10.21.5.98 255.255.255.248
S1(config-if)#ipv6 add 2001:db8:acad:c::98/64
S1(config-if)#ipv6 add fe80::98 link-local
S1(config-if)#no shutdown
S1(config-if)#exit

S1(config)#ip default-gateway 10.21.5.97

```

### **Comandos para configurar S2:**

```

Switch(config)#no ip domain-lookup

Switch(config)#hostname S2

S2(config)#ip domain-name ccna-lab.com

S2(config)#enable secret ciscoenpass

S2(config)#line con 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit

```

```
S2(config)#username admin privilege 15 secret adminlpass
```

```
S2(config)#line vty 0 15
S2(config-line)#transport input ssh
S2(config-line)#login local
S2(config-line)#exit
```

```
S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#exit
```

```
S2(config)#service password-encryption
```

```
S2(config)#banner motd "ACCESO NO AUTORIZADO".
```

```
S2(config)#crypto key generate rsa
```

```
S2(config)#interface vlan 4
S2(config-if)#ip add 10.21.5.99 255.255.255.248
S2(config-if)#ipv6 add 2001:db8:acad:c::99/64
S2(config-if)#ipv6 add fe80::99 link-local
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 10.21.5.97
```

## Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

### Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 5. Tareas de configuración VLAN y troncales para el Switch S1

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

### Comandos para configurar S1:

```

S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1#configure terminal
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1#configure terminal
S1(config)#interface fa0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#interface fa0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit

S1(config)#interface range fa0/1-2
S1(config-if-range)#channel-group
2 mode active
S1(config)#exit
S1(config)#interface port-channel 2
S1(config-if)#switchport mode trunk

```

```

S1(config)#switchport trunk native vlan 6

S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#no shutdown
S1(config-if)#exit

S1(config)#interface fa0/6
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3

S1(config)#interface range fa0/3-
4, fa0/7-24, gi0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description
Puertos sin utilizar
S1(config-if-range)#shutdown

```

#### Paso 5: Configure el S2.

Entre las tareas de configuración de S2 se incluyen las siguientes:

Tabla 6. Tareas de configuración Switch S2

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18

Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

## Comandos para configurar S2:

```

S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native

S2(config)#interface range fa0/1-2
S2(config-if-range)#switchport
mode trunk

S2(config)#interface port
S2(config)#interface port-channel 2
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#interface range fa0/1-2 channel-group 2 mode passive
S2(config-if-range)#no shutdown

S2(config)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit

S2(config)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3

S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5

```

```
S2(config-if-range)#description "SIN UTILIZAR"
S2(config-if-range)#shutdown
```

## Parte 2: Configurar soporte de host.

### Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 7. Configuración de R1 DHCP

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

### Comandos para configurar R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 lo0

R1#configure terminal
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.21.5.0 255.255.255.192
R1(dhcp-config)#default-router 10.21.5.1
R1(dhcp-config)#domain-name CCNA-a.net
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.21.5.2 10.21.5.51
```

## Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 8. Network PC-A

<b>PC-A Network Configuración</b>	
Descripción	ccna-a.net
Dirección física	00D0.FFBD.6E53
Dirección IP	10.21.5.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Tabla 9. Network PC-B

<b>Configuración de red de PC-B</b>	
Descripción	ccna-b.net
Dirección física	0001.C9C0.A2C3
Dirección IP	169.254.162.195
Máscara de subred	255.255.0.0
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

## Parte 3: Probar y verificar la conectividad de extremo a extremo.

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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:



<b>Desde</b>	<b>A</b>	<b>de Internet</b>	<b>Dirección IP</b>	<b>Resultados de ping</b>
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	
PC-A	R1, G0/0/1.2	IPv6	2001:db5:acad:a: :1	
PC-A	R1, G0/0/1.3	Dirección	10.21.5.65	
PC-A	R1, G0/0/1.3	IPv6	2001:db5:acad:b: :1	
PC-A	R1, G0/0/1.4	Dirección	10.21.5.97	
PC-A	R1, G0/0/1.4	IPv6	2001:db5:acad:c: :1	
PC-A	S1, VLAN 4	Dirección	10.21.5.98	
PC-A	S1, VLAN 4	IPv6	2001:db5:acad:c: :98	
PC-A	S2, VLAN 4	Dirección	10.21.5.99.	
PC-A	S2, VLAN 4	IPv6	2001:db5:acad:c: :99	
PC-A	PC-B	Dirección	IP address will vary.	
PC-A	PC-B	IPv6	2001:db5:acad:b: :50	
PC-A	R1 Bucle 0	Dirección	209.165.201.1	
PC-A	R1 Bucle 0	IPv6	2001:db5:acad:209: :1	
PC-B	R1 Bucle 0	Dirección	209.165.201.1	
PC-B	R1 Bucle 0	IPv6	2001:db5:acad:209: :1	
PC-B	R1, G0/0/1.2	Dirección	10.21.5.1	
PC-B	R1, G0/0/1.2	IPv6	2001:db5:acad:a: :1	
PC-B	R1, G0/0/1.3	Dirección	10.21.5.65	
PC-B	R1, G0/0/1.3	IPv6	2001:db5:acad:b: :1	
PC-B	R1, G0/0/1.4	Dirección	10.21.5.97	
PC-B	R1, G0/0/1.4	IPv6	2001:db5:acad:c: :1	
PC-B	S1, VLAN 4	Dirección	10.21.5.98	
PC-B	S1, VLAN 4	IPv6	2001:db5:acad:c: :98	
PC-B	S2, VLAN 4	Dirección	10.21.5.99.	
PC-B	S2, VLAN 4	IPv6	2001:db5:acad:c: :99	

Figura 2. Ping PC-A a R1, G0/1.2

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.21.5.1

Pinging 10.21.5.1 with 32 bytes of data:

Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db5:acad:a::1
Invalid Command.

C:\>ping 2001:db5:acad:a::1

Pinging 2001:db5:acad:a::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time=3ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>
```

Figura 3. Ping desde PC-A a R1, G0/0/1.3

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.65

Pinging 10.21.5.65 with 32 bytes of data:

Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db5:acad:b::1

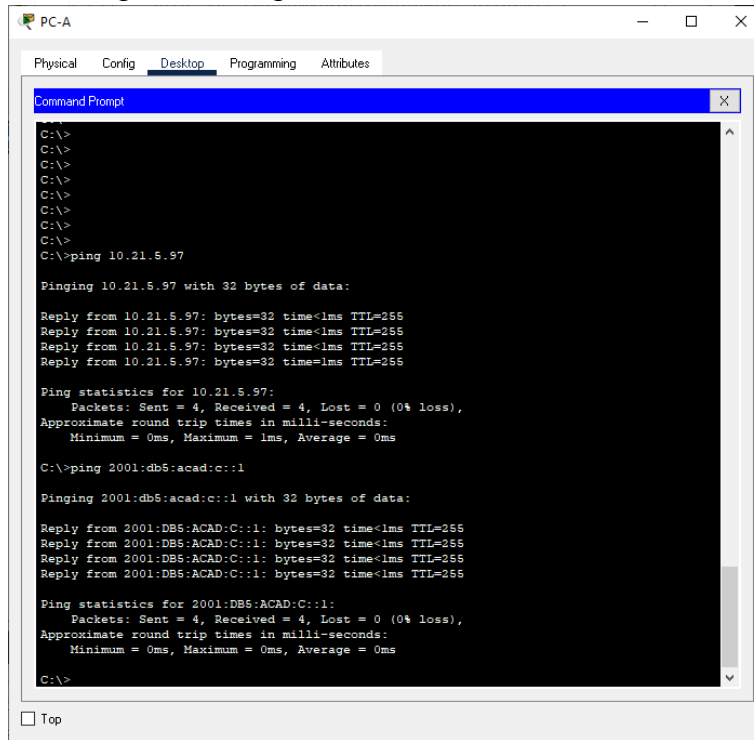
Pinging 2001:db5:acad:b::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:B::1: bytes=32 time=8ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Figura 4. Ping desde PC-A a R1, G0/0/1.4



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.97

Pinging 10.21.5.97 with 32 bytes of data:

Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db5:acad:c::1

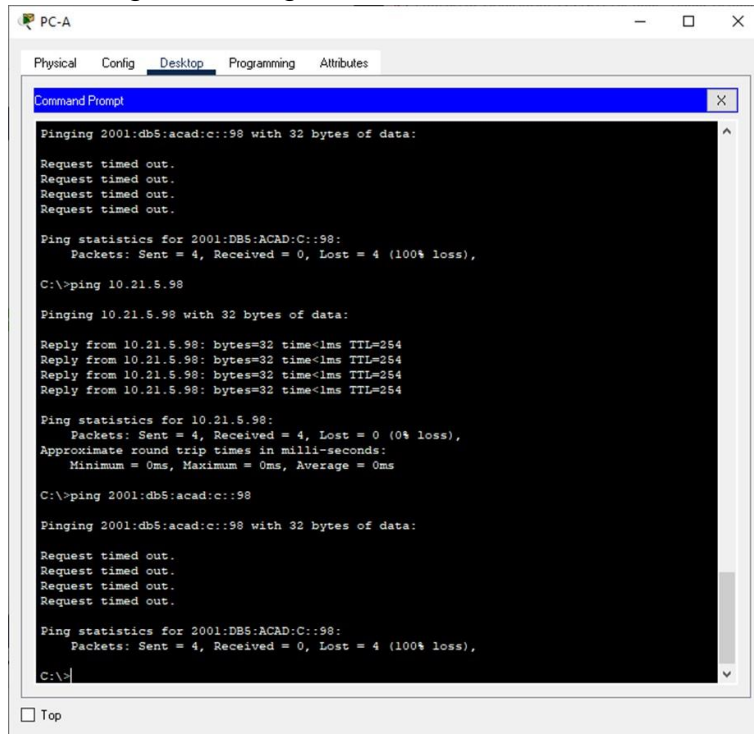
Pinging 2001:db5:acad:c::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 5. Ping desde PC-A a S1, VLAN 4



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 2001:db5:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.21.5.98

Pinging 10.21.5.98 with 32 bytes of data:

Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db5:acad:c::98

Pinging 2001:db5:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figura 6. Ping desde PC-A a S2, VLAN 4

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.99
Pinging 10.21.5.99 with 32 bytes of data:
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time=1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time=1ms TTL=254
Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db5:acad:c::99
Pinging 2001:db5:acad:c::99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB5:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 7. Ping desde PC-A a PC-B.

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.84
Pinging 10.21.5.84 with 32 bytes of data:
Reply from 10.21.5.84: bytes=32 time<1ms TTL=127
Reply from 10.21.5.84: bytes=32 time=12ms TTL=127
Reply from 10.21.5.84: bytes=32 time=10ms TTL=127
Reply from 10.21.5.84: bytes=32 time=14ms TTL=127
Ping statistics for 10.21.5.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 9ms
C:\>
```

Figura 8. Ping desde PC-B a R1 Bucle 0

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 9. Ping desde PC-B a R1, G0/0/1.2

```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.1

Pinging 10.21.5.1 with 32 bytes of data:

Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255
Reply from 10.21.5.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:a::1

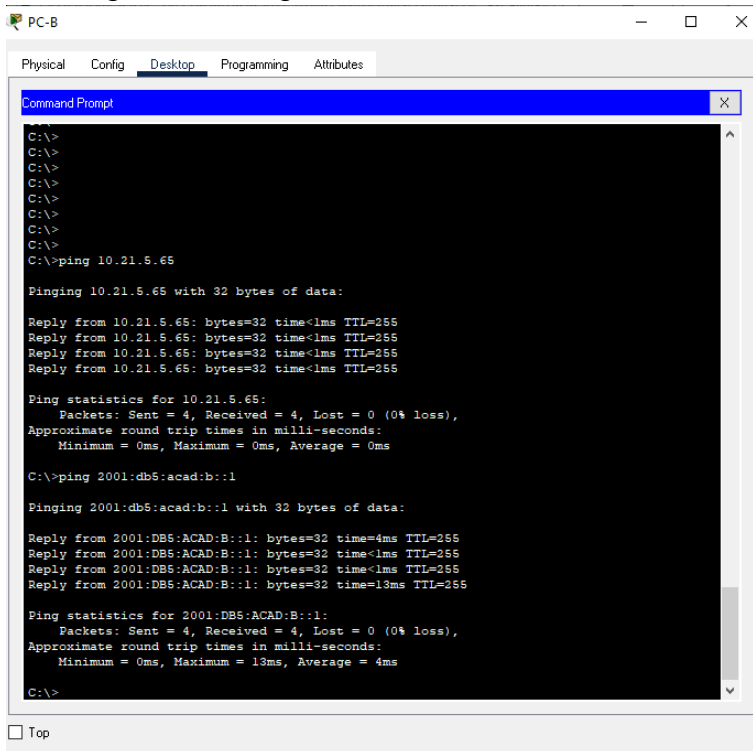
Pinging 2001:db8:acad:a::1 with 32 bytes of data:

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

C:\>
```

Figura 10. Ping desde PC-B a R1, G0/0/1.3



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.65

Pinging 10.21.5.65 with 32 bytes of data:

Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255
Reply from 10.21.5.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db5:acad:b::1

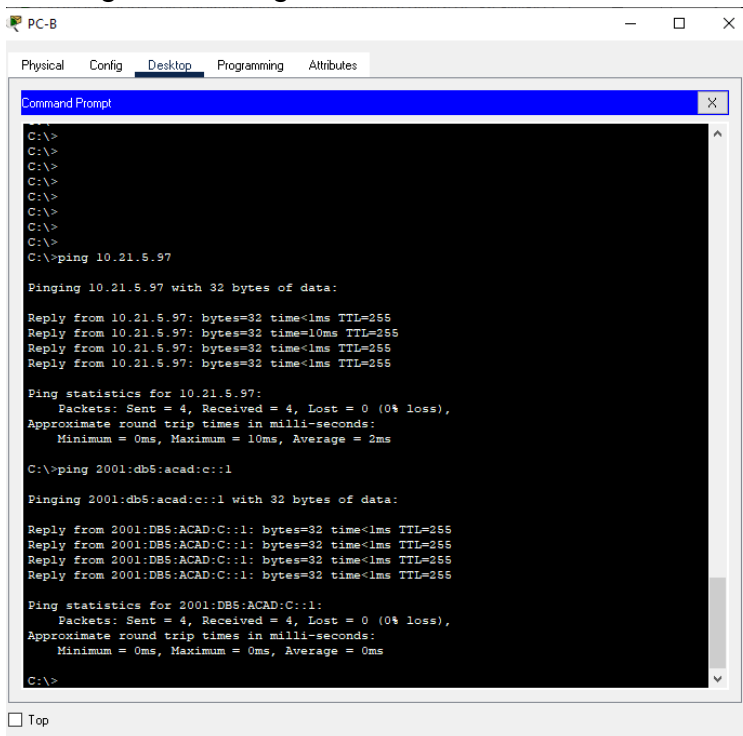
Pinging 2001:db5:acad:b::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:B::1: bytes=32 time=4ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:B::1: bytes=32 time=13ms TTL=255

Ping statistics for 2001:DB5:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 4ms

C:\>
```

Figura 11. Ping desde PC-B a R1, G0/0/1.4



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.97

Pinging 10.21.5.97 with 32 bytes of data:

Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time=10ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255
Reply from 10.21.5.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.21.5.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 2001:db5:acad:c::1

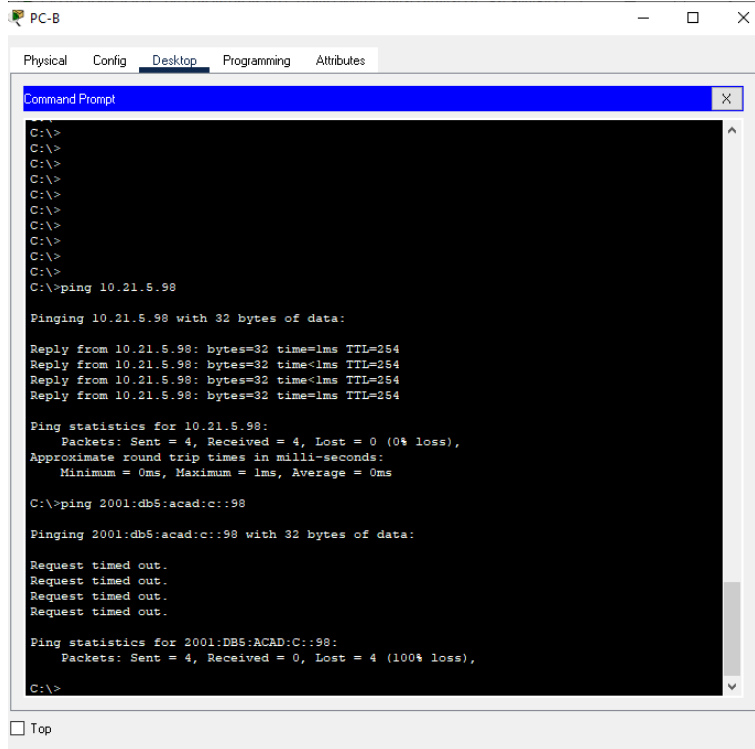
Pinging 2001:db5:acad:c::1 with 32 bytes of data:

Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB5:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB5:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 12. Ping desde PC-B a S1, VLAN 4



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.98

Pinging 10.21.5.98 with 32 bytes of data:

Reply from 10.21.5.98: bytes=32 time=1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time<1ms TTL=254
Reply from 10.21.5.98: bytes=32 time=1ms TTL=254

Ping statistics for 10.21.5.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db5:acad:c::98

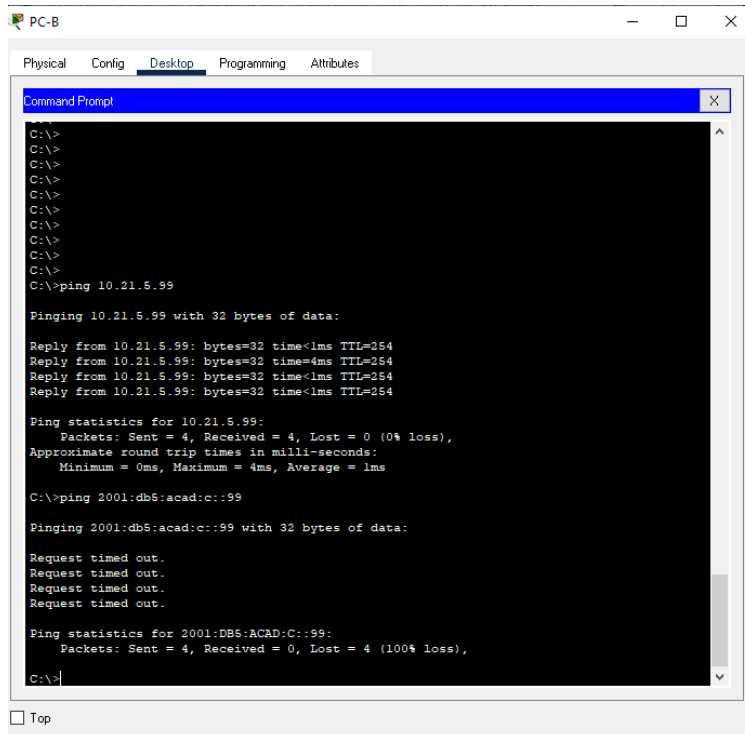
Pinging 2001:db5:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figura 13. Ping desde PC-B a S2, VLAN 4.



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.21.5.99

Pinging 10.21.5.99 with 32 bytes of data:

Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time=4ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254
Reply from 10.21.5.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.21.5.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 2001:db5:acad:c::99

Pinging 2001:db5:acad:c::99 with 32 bytes of data:

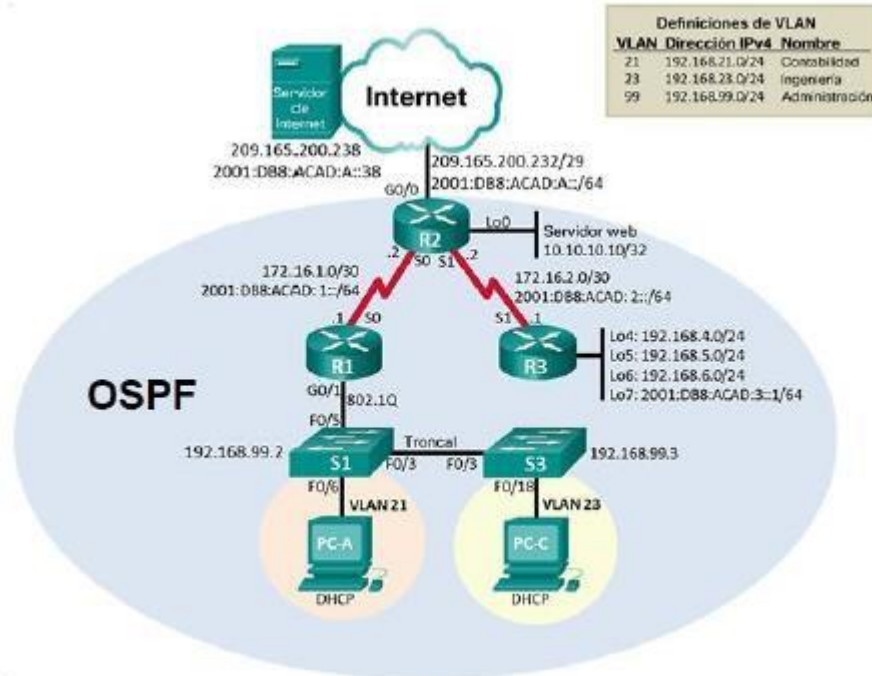
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB5:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## ESCENARIO 2

Figura 14. Topología 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.

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.



## Comandos:

### Eliminar el archivo startup-config de todos los routers

```
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#
```

### Volver a cargar todos los routers

```
Router#reload
Proceed with reload? [confirm]
```

### Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

```
Switch>enable
Switch#erase sta
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

### Volver a cargar ambos switches

```
Switch#reload
Proceed with reload? [confirm]
```

### Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

```
Switch>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#
```

## 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 10. Configuración de la computadora 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	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::2/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

### Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Comandos:

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 "ACCESO NO AUTORIZADO"
```

### Interfaz S0/0/0

```
R1(config)#interface serial 0/0/0
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 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#ipv6 unicast
R1(config)#ipv6 unicast-routing
R1(config)#
```

## Paso 3: Configurar R2

### La configuración del R2 incluye las siguientes tareas:

#### Comandos:

#### 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
```

### Mensaje MOTD

```
R2(config)#banner motd "ACCESO NO AUTORIZADO"
```

### Interfaz S0/0/0

```
R2(config)#interface serial 0/0/0
R2(config-if)#description R1 a R2
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

### Interfaz G0/0 (simulación de internet)

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#description R2 to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#exit
```

### Interfaz loopback 0 (servidor web simulado)

```
R2(config)#interface lo0
R2(config-if)#
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
```

### Rutas predeterminadas

```
R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0
R2(config)#ipv6 route ::/0 gigabitEthernet 0/0
R2(config)#ipv6 unicast
```

```
R2 (config) #ipv6 unicast-routing
R2 (config) #
```

#### **Paso 4: Configurar R3**

**La configuración del R3 incluye las siguientes tareas:**

Comandos:

##### **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 "ACCESO NO AUTORIZADO"
```

### **Interfaz S0/0/1**

```
R3(config)#interface serial 0/0/1
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
R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#
```

### **Rutas predeterminadas**

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
```

## **Paso 5: Configurar S1**

**La configuración del S1 incluye las siguientes tareas:**

Comandos:

### **Desactivar la búsqueda DNS**

```
Router(config)#no ip domain-lookup
```

### **Nombre del router**

```
Router(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 4  
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 "ACCESO NO AUTORIZADO"
```

## **Paso 6: Configurar el S3**

**La configuración del S3 incluye las siguientes tareas:**

Comandos:

### **Desactivar la búsqueda DNS**

```
Router(config)#no ip domain-lookup
```

### **Nombre del router**

```
Router(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 4  
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 "ACCESO NO AUTORIZADO"
```



**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 11. Verificación de la conectividad de los dispositivos.

<b>Desde</b>	<b>A</b>	<b>Dirección IP</b>	<b>Resultados de ping</b>
R1	R2, S0/0/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), 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
----------------	------------------------	-----------------	--

### **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:

Comandos:

##### **Crear la base de datos de VLAN**

```
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
```

##### **Asignar la dirección IP de administración.**

```
S1(config)#interface vlan 99
S1(config-if)#
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
```

##### **Asignar el gateway predeterminado**

```
S1(config)#ip default-gateway 192.168.99.1.
```

##### **Forzar el enlace troncal en la interfaz F0/3**

```
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

##### **Forzar el enlace troncal en la interfaz F0/5**

```
S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```

##### **Configurar el resto de los puertos como puertos de acceso**

```
S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

### Asignar F0/6 a la VLAN 21

```
S1(config)#interface range fa0/6
S1(config-if-range)#switchport access vlan 21
S1(config-if-range)#exit
```

### Apagar todos los puertos sin usar

```
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

## Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

### Comandos:

#### Crear la base de datos de VLAN

```
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
```

#### Asignar la dirección IP de administración.

```
S3(config)#interface vlan 99
S3(config-if)#
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
```

#### Asignar el gateway predeterminado

```
S3(config)#ip default-gateway 192.168.99.1
```

#### Forzar el enlace troncal en la interfaz F0/3

```
S3(config)#interface fastEthernet 0/3
S3(config-if)#
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
```

### Configurar el resto de los puertos como puertos de acceso

```
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

### Asignar F0/6 a la VLAN 21

```
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
```

### Apagar todos los puertos sin usar

```
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
```

## Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

### Comandos:

#### Configurar la subinterfaz 802.1Q .21 en G0/1

```
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
```

#### Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1(config)#interface gigabitEthernet 0/1.23
R1(config-subif)#description accounting LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
```

#### Configurar la subinterfaz 802.1Q .99 en G0/1

```
R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#description accounting LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
```

#### Activar la interfaz G0/1

```
R1 (config) #interface gigabitEthernet 0/1
R1 (config-if) #no shutdown
R1 (config-if) #exit
```

#### 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 12. Conectividad de la red

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 80 percent (4/5), 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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S1	R1, dirección VLAN 21	192.168.21.1	S1#ping 192.168.21.1  Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
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

Figura 15. Comandos de ping desde S1

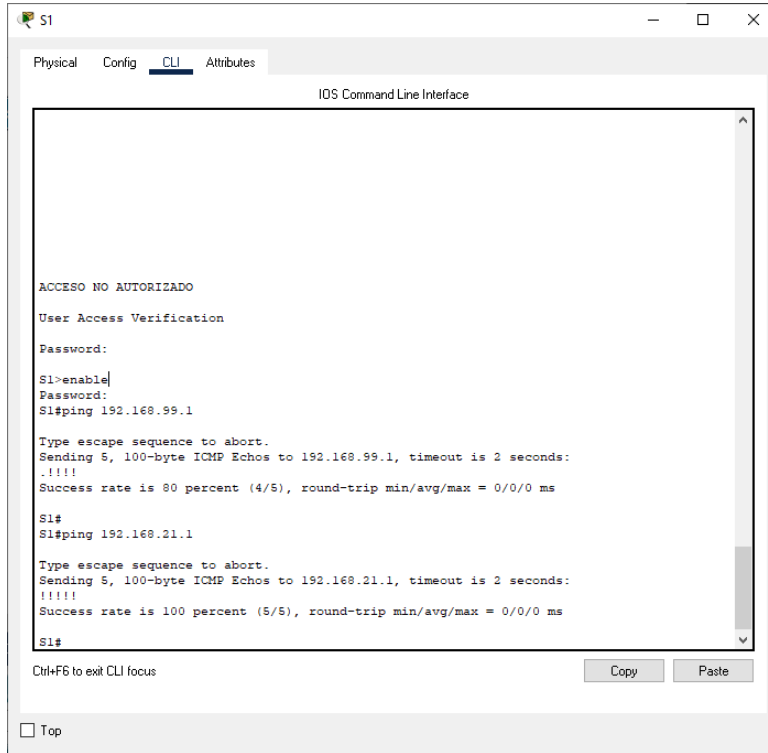
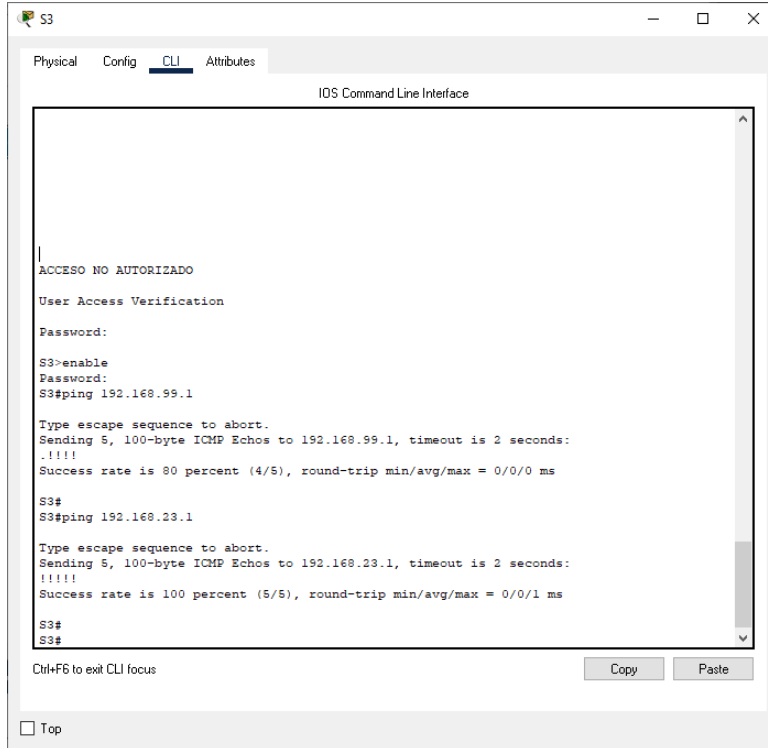


Figura 16. Comandos de ping desde S3





## 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:

Comandos:

#### 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 gi0/1.21
R1(config-router)#passive-interface gi0/1.23
R1(config-router)#passive-interface gi0/1.99
```

#### Desactive la sumarización automática

```
R1(config-router)#no auto-summary
```

### Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

#### 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 todas las interfaces LAN como pasivas

```
R2(config-router)#passive-interface lo0
```

#### Desactive la sumarización automática

```
R2(config-router)#no auto-summary
```

### Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

#### 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
```

### 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 13. Verificación de la información de OSPF

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

Figura 17. Comando de “show ip protocols” en R1.

```

R1
-----
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:
R1>enable
Password:
R1#
R1#show ip proto
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):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:17:35
    192.168.6.1      110          00:17:34
    192.168.99.1     110          00:21:33
  Distance: (default is 110)

R1#
R1#
-----
Ctrl+F6 to exit CLI focus          Copy      Paste
-----
 Top

```

Figura 18. Comando de “show ip route ospf” en R1.

```

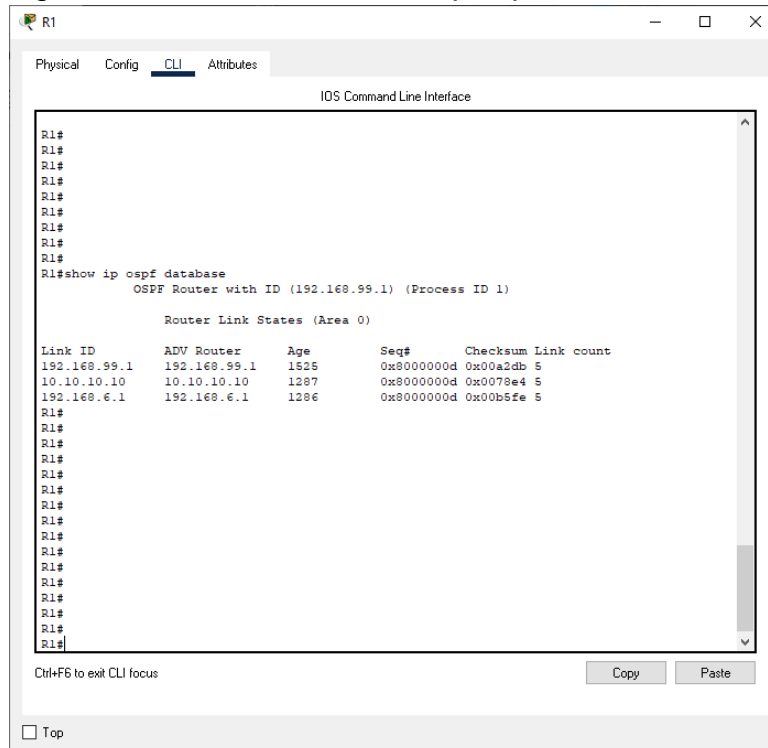
R1
-----
Physical Config CLI Attributes
IOS Command Line Interface

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#show ip route ospf
  10.0.0.0/32 is subnetted, 1 subnets
O    10.10.10.10 [110/65] via 172.16.1.2, 04:25:16, Serial0/0/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O    172.16.2.0 [110/120] via 172.16.1.2, 04:25:16, Serial0/0/0
  192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.1 [110/129] via 172.16.1.2, 04:21:03, Serial0/0/0
  192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.1 [110/129] via 172.16.1.2, 04:21:03, Serial0/0/0
  192.168.6.0/32 is subnetted, 1 subnets
O    192.168.6.1 [110/129] via 172.16.1.2, 04:21:03, Serial0/0/0

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
-----
Ctrl+F6 to exit CLI focus          Copy      Paste
-----
 Top

```

Figura 19. Comando de “show ip ospf database” en R1.

The image shows a terminal window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, showing an 'IOS Command Line Interface'. The terminal output displays the command 'R1#show ip ospf database' and its output for an OSPF Router with ID (192.168.99.1) in Process ID 1. The output shows 'Router Link States (Area 0)' with a table of Link ID, ADV Router, Age, Seq#, Checksum, and Link count.

```
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
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  1525         0x8000000d    0x00a2db 5
10.10.10.10    10.10.10.10   1287         0x8000000d    0x0078e4 5
192.168.6.1    192.168.6.1   1286         0x8000000d    0x00b5fe 5

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

**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:

Comandos:

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

```
R1(config)#ip dhcp excluded-address 192.168.21.1  
192.168.21.30
```

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

```
R1(config)#ip dhcp excluded-address 192.168.23.1  
192.168.23.30
```

### Crear un pool de DHCP para la VLAN 21

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
```

### Crear un pool de DHCP para la VLAN 23

```
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
```

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

La configuración del R2 incluye las siguientes tareas:

Comandos:

Crear una base de datos local con una cuenta de usuario

```
R2(config)#user webuser privilege 15 secret cisco12345
```

Habilitar el servicio del servidor HTTP

No soporta

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

No 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
R2(config-if)#ip nat inside
```

Configurar la NAT dinámica dentro de una ACL privada

```
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
```

Defina el pool de direcciones IP públicas utilizables.

```
R2(config)#ip nat pool INTERNET 209.165.200.232  
209.165.200.237 netmask 255.255.255.248
```

Definir la traducción de NAT dinámica

```
R2(config)#ip nat inside source list 1 pool INTERNET
```

### 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.

Figura 20. Configuración PC-A

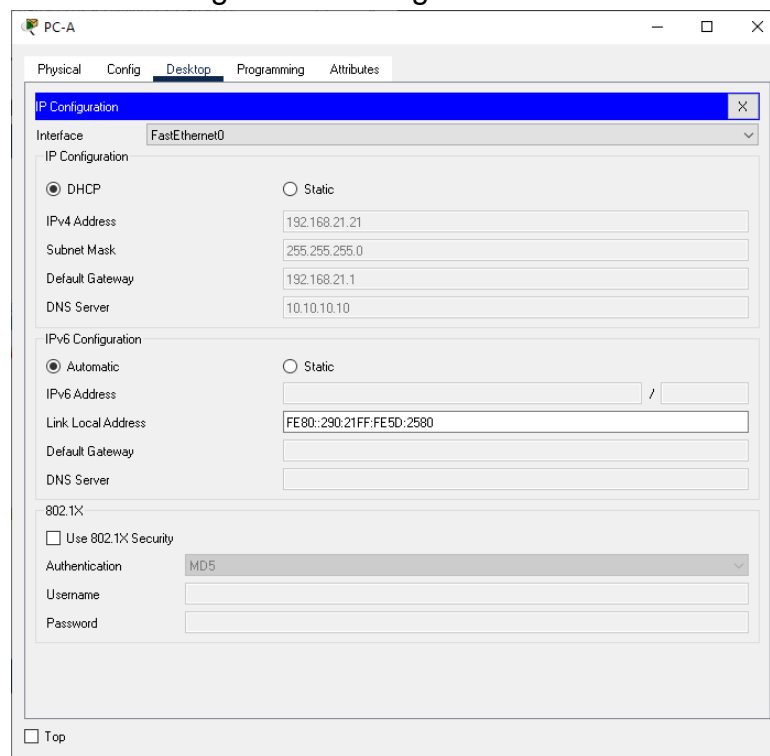


Figura 21. Configuración PC-C

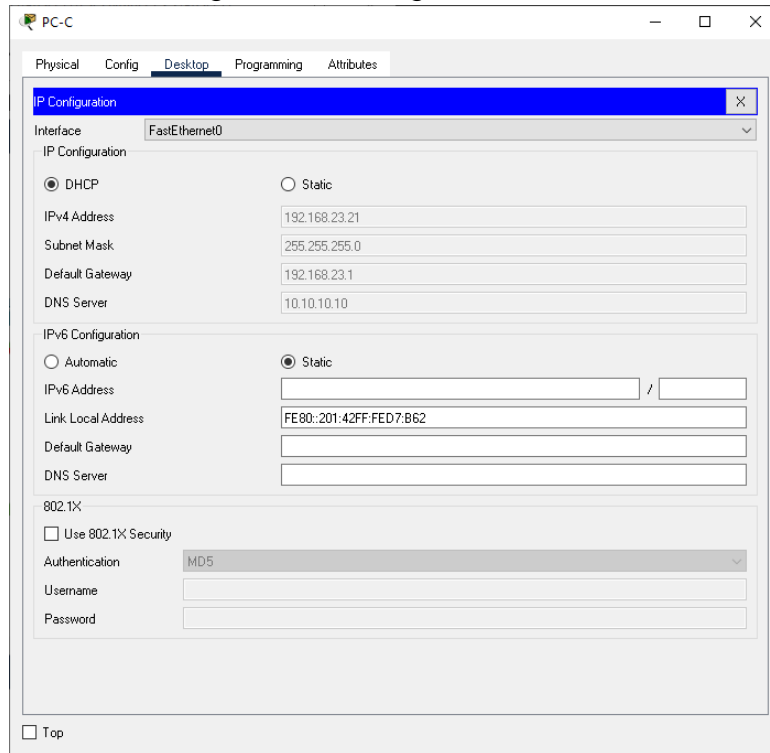
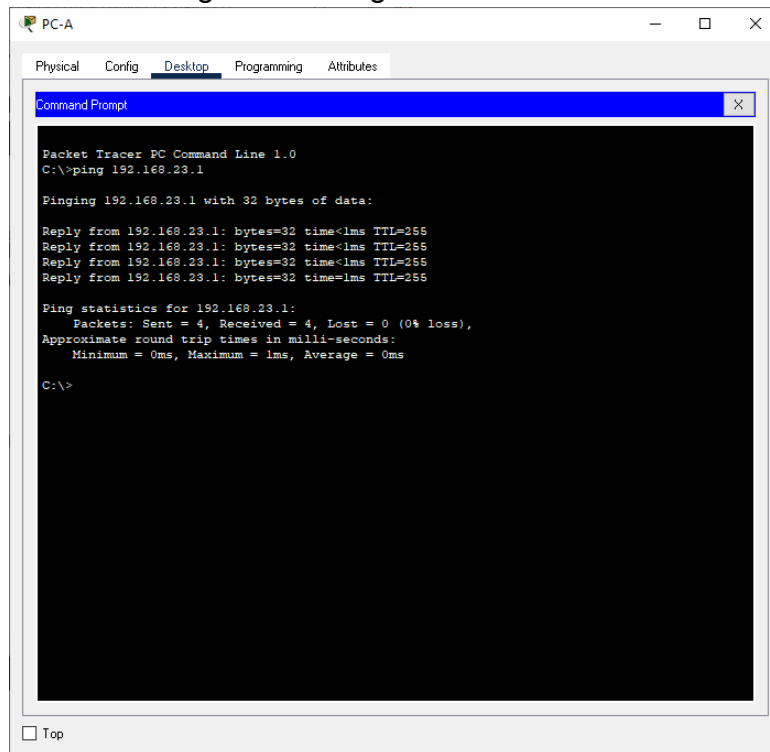


Figura 22. Ping de PC-A a PC-C







```
R2(config)#ip access-list standard ADMIN-MGT
```

Aplicar la ACL con nombre a las líneas VTY

Permitir acceso por Telnet a las líneas de VTY

```
R2(config-std-nacl)#permit host 172.16.1.1
```

```
R2(config-std-nacl)#exit
```

Verificar que la ACL funcione como se espera

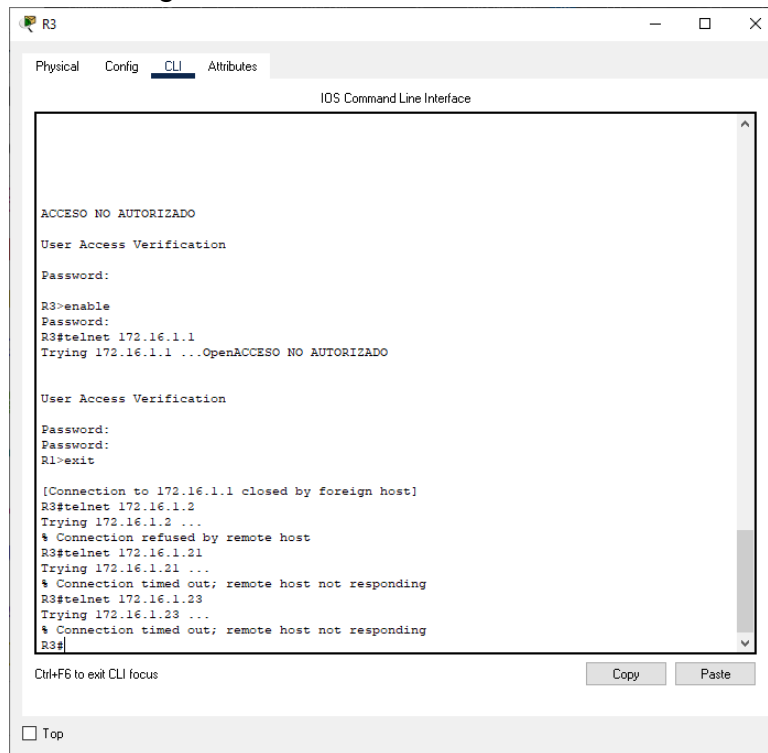
```
R2(config)#line vty 0 4
```

```
R2(config-line)#access
```

```
R2(config-line)#access-class ADMIN-MGT in
```

```
R2(config-line)#exit
```

Figura 25. Funcionamiento de la ACL.



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

Tabla 15. Comandos de verificación.

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 <b>Nota:</b> 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

## CONCLUSIÓN

Con las prácticas y conocimientos adquiridos, se culmina la actividad cumpliendo con los objetivos, configurando los dispositivos de una pequeña red en el software de simulación Packet Tracer, se realizan los enrutamientos entre VLAN, DHCP, Etherchannel y port-security, comprobando con los comandos “ping, ipconfig /all, tracert”.

## BIBLIOGRAFÍA

CISCO Networking Academy. Capitulo 5 Ethernet. Recuperado de:  
<https://contenthub.netacad.com/legacy/CCNA/ITN/6.0/es/index.html#5.1.1.1>

Definiciones (2020). DNS. Recuperado de:  
<https://definicion.de/dns/#:~:text=La%20sigla%20DNS%20proviene%20de,Protocolo%20de%20Internet>).

Redes de computador (2018). Dispositivos enrutadores: Routers. Recuperado de:  
[http://redesdecomputadores.umh.es/red/routers/default.html#:~:text=El%20router%20\(enrutador%20o%20encaminador,de%20red%20o%20redes%20enteras](http://redesdecomputadores.umh.es/red/routers/default.html#:~:text=El%20router%20(enrutador%20o%20encaminador,de%20red%20o%20redes%20enteras).

Redes Zone (2019). VLANs: Qué son, tipos y para que sirven. Recuperado de:  
<https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/>.

# DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Luis Mateo Cruz Gil

Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería

ECBTI.

Pereira, Colombia

[lmacruzgi@unadvirtual.edu.co](mailto:lmacruzgi@unadvirtual.edu.co)

## RESUMEN

El presente trabajo es una de las actividades evaluativas que tiene el diplomado de profundización CCNA de la empresa de CISCO, donde demostramos los conocimientos adquiridos durante todo el proceso formativo que tiene. Este se divide en dos escenarios.

Escenario uno, se configuran un grupo de dispositivos que lo conforman dos switches, un router y dos PC con el objetivo de conectarlos a través de IPv4 e IPv6, esta red es administrable y con niveles de seguridad, los enrutamientos son con VLAN y DHCP.

**PALABRAS CLAVES:** Dispositivos, CISCO, Seguridad, Conexión.

## ABSTRACT

The present work is one of the evaluative activities that the CISCO company CCNA deepening diploma has, where we demonstrate the knowledge acquired throughout the training process that it has. This is divided into two scenarios.

Scenario one, a group of devices is configured that is made up of two switches, a router and two PCs in order to connect them through IPv4 and IPv6,

this network is manageable and with security levels, the routing is with VLAN and DHCP.

**KEY WORDS:** Devices, CISCO, Security, Connection.

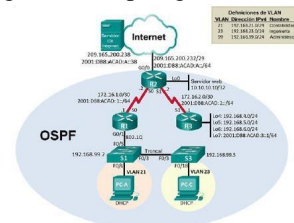
## INTRODUCCION

En este trabajo se encuentra el desarrollo paso a paso de las actividades que indica el segundo escenario del diplomado, están las evidencias del uso del software Packet Tracer y se documentan los comandos que se utilizan para la configuración y prueba de los dispositivos de la red que se simula.

Culminando esta actividad se da a conocer las competencias y habilidades que generan las estrategias de aprendizaje que se implementaron para realizar cada una de las actividades de las que se compone este diplomado.

## ESCENARIO 2

Figura 14. Topología 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.

### 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.

Comandos:

Eliminar el archivo startup-config de todos los routers

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#

Volver a cargar todos los routers

Router#reload

Proceed with reload? [confirm]

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

Switch>enable

Switch#erase sta

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

Volver a cargar ambos switches

Switch#reload

Proceed with reload? [confirm]

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Switch>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#

### 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 10. Configuración de la computadora 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	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::2/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

## Paso 2: Configurar R1

### Las tareas de configuración para R1 incluyen las siguientes:

Comandos:

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 "ACCESO NO AUTORIZADO"

Interfaz S0/0/0

R1(config)#interface serial 0/0/0

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 s0/0/0

R1(config)#ipv6 route ::/0 s0/0/0

R1(config)#ipv6 unicast

R1(config)#ipv6 unicast-routing

R1(config)#

## Paso 3: Configurar R2

### La configuración del R2 incluye las siguientes tareas:

Comandos:

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup	R2(config-if)#ip address 172.16.1.2 255.255.255.252
Nombre del router	R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
Router(config)#hostname R2	R2(config-if)#no shutdown
Contraseña de exec privilegiado cifrada	R2(config-if)#exit
R2(config)#enable secret class	Interfaz G0/0 (simulación de internet)
Contraseña de acceso a la consola	R2(config)#interface gigabitEthernet 0/0
R2(config)#line con 0	R2(config-if)#description R2 to Internet
R2(config-line)#password cisco	R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-line)#login	R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-line)#exit	R2(config-if)#no shutdown
Contraseña de acceso Telnet	R2(config-if)#
R2(config)#line vty 0 4	R2(config-if)#exit
R2(config-line)#password cisco	Interfaz loopback 0 (servidor web simulado)
R2(config-line)#login	R2(config)#interface lo0
R2(config-line)#exit	R2(config-if)#
Cifrar las contraseñas de texto no cifrado	R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config)#service password-encryption	R2(config-if)#exit
Mensaje MOTD	Rutas predeterminadas
R2(config)#banner motd "ACCESO NO AUTORIZADO"	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0
Interfaz S0/0/0	R2(config)#ipv6 route ::/0 gigabitEthernet 0/0
R2(config)#interface serial 0/0/0	R2(config)#ipv6 unicast-routing
R2(config-if)#description R1 a R2	R2(config)#



#### **Paso 4: Configurar R3**

**La configuración del R3 incluye las siguientes tareas:**

Comandos:

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 "ACCESO NO AUTORIZADO"

Interfaz S0/0/1

R3(config)#interface serial 0/0/1

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

R3(config-if)#exit

R3(config)#ipv6 unicast-routing

R3(config)#

Rutas predeterminadas

R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

R3(config)#ipv6 route ::/0 s0/0/1

### **Paso 5: Configurar S1**

**La configuración del S1 incluye las siguientes tareas:**

Comandos:

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Nombre del router

Router(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 4

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 "ACCESO NO  
AUTORIZADO"

### **Paso 6: Configurar el S3**

**La configuración del S3 incluye las siguientes tareas:**

Comandos:

Desactivar la búsqueda DNS

Router(config)#no ip domain-lookup

Nombre del router

Router(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 4

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 "ACCESO NO AUTORIZADO"

### 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 11. Verificación de la conectividad de los dispositivos.

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

			!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/9 ms
R2	R3, S0/0/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), 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
----------------	------------------------	-----------------	---

			<p>Reply from 2001:DB8:AC AD:A::1: bytes=32 time=1ms TTL=255</p> <p>Ping statistics for 2001:DB8:AC AD:A::1:</p> <p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</p> <p>Approximate round trip times in milliseconds:</p> <p>Minimum = 0ms, Maximum = 1ms, Average = 0ms</p>
--	--	--	--

### 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:

Comandos:

Crear la base de datos de VLAN

```
S1(config)#vlan 21
```

```
S1(config-vlan)#name Contabilidad
```

```
S1(config-vlan)#vlan 23
```

```
S1(config-vlan)#name Ingenieria
```

```
S1(config-vlan)#vlan 99
```

```
S1(config-vlan)#name Administracion
```

```
S1(config-vlan)#exit
```

Asignar la dirección IP de administración.

```
S1(config)#interface vlan 99
```

```
S1(config-if)#
```

```
S1(config-if)#ip address 192.168.99.2  
255.255.255.0
```

```
S1(config-if)#exit
```

Asignar el gateway predeterminado

```
S1(config)#ip default-gateway 192.168.99.1.
```

Forzar el enlace troncal en la interfaz F0/3

```
S1(config)#interface fastEthernet 0/3
```

```
S1(config-if)#switchport mode trunk
```

```
S1(config-if)#
```

```
S1(config-if)#switchport trunk native vlan 1
```

```
S1(config-if)#exit
```

Forzar el enlace troncal en la interfaz F0/5

```
S1(config)#interface fastEthernet 0/5
```

```
S1(config-if)#switchport mode trunk
```

```
S1(config-if)#switchport trunk native vlan 1
```

```
S1(config-if)#exit
```

Configurar el resto de los puertos como puertos de acceso

```
S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24
```

```
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#exit
```

Asignar F0/6 a la VLAN 21

```
S1(config)#interface range fa0/6
S1(config-if-range)#switchport access vlan 21
S1(config-if-range)#exit
```

Apagar todos los puertos sin usar

```
S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#exit
```

## **Paso 2: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

Comandos:

Crear la base de datos de VLAN

```
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
```

Asignar la dirección IP de administración.

```
S3(config)#interface vlan 99
S3(config-if)#
S3(config-if)#ip address 192.168.99.3
255.255.255.0
S3(config-if)#exit
```

Asignar el gateway predeterminado

```
S3(config)#ip default-gateway 192.168.99.1
```

Forzar el enlace troncal en la interfaz F0/3

```
S3(config)#interface fastEthernet 0/3
S3(config-if)#
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
```

Configurar el resto de los puertos como puertos de acceso

```
S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

Asignar F0/6 a la VLAN 21

```
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
```

Apagar todos los puertos sin usar

```
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2
S3(config-if-range)#shutdown
S3(config-if-range)#exit
```

## **Paso 3: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

R1(config-if)#exit

Comandos:

Configurar la subinterfaz 802.1Q .21 en G0/1

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

Configurar la subinterfaz 802.1Q .23 en G0/1

R1(config)#interface gigabitEthernet 0/1.23

R1(config-subif)#description accounting LAN de Ingenieria

R1(config-subif)#encapsulation dot1q 23

R1(config-subif)#ip address 192.168.23.1 255.255.255.0

R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .99 en G0/1

R1(config)#interface gigabitEthernet 0/1.99

R1(config-subif)#description accounting LAN de Administracion

R1(config-subif)#encapsulation dot1q 99

R1(config-subif)#ip address 192.168.99.1 255.255.255.0

R1(config-subif)#exit

Activar la interfaz G0/1

R1(config)#interface gigabitEthernet 0/1

R1(config-if)#no shutdown

#### 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 12. Conectividad de la red

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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

S3	R1, dirección VLAN 99	192.168.99.1	<p>S3#ping 192.168.99.1</p> <p>Type escape sequence to abort.</p> <p>Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:</p> <p>!!!!</p> <p>Success rate is 80 percent (4/5), round- trip min/avg/max = 0/0/0 ms</p>
----	--------------------------------	--------------	--

Figura 15. Comandos de ping desde S1

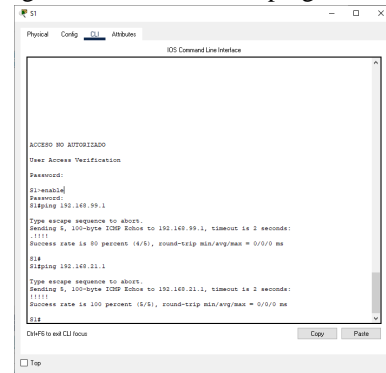
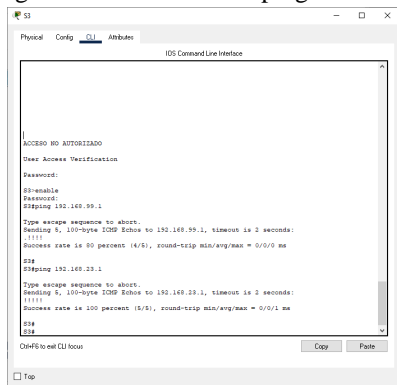


Figura 16. Comandos de ping desde S3



#### 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:

Comandos:

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 gi0/1.21
```

```
R1(config-router)#passive-interface gi0/1.23
```

```
R1(config-router)#passive-interface gi0/1.99
```

Desactive la sumariación automática

```
R1(config-router)#no auto-summary
```

##### Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

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 todas las interfaces LAN como pasivas

```
R2(config-router)#passive-interface lo0
```

Desactive la sumariación automática

```
R2(config-router)#no auto-summary
```

##### Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

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
```

#### 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 13. Verificación de la información de OSPF

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

OSPF de la configuración en ejecución?

Figura 17. Comando de “show ip protocols” en R1.

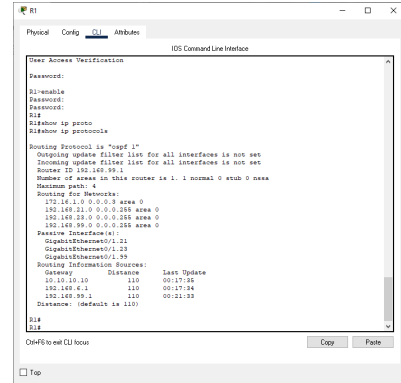


Figura 18. Comando de “show ip route ospf” en R1.

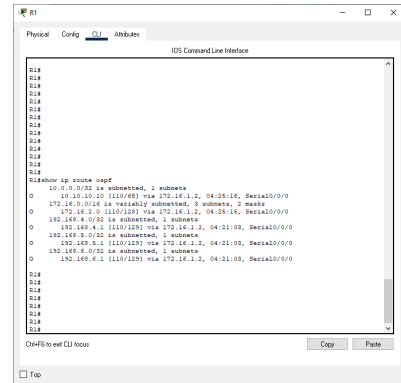
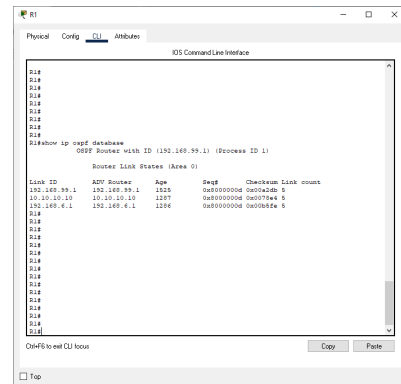


Figura 19. Comando de “show ip ospf database” en R1.



## 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:

Comandos:

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

```
R1(config)#ip dhcp excluded-address  
192.168.21.1 192.168.21.30
```

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

```
R1(config)#ip dhcp excluded-address  
192.168.23.1 192.168.23.30
```

Crear un pool de DHCP para la VLAN 21

```
R1(config)#ip dhcp pool ACCT  
  
R1(dhcp-config)#dns-server 10.10.10.10  
R1(dhcp-config)#domain-name ccna-sa.com  
R1(dhcp-config)#default-router 192.168.21.1  
  
R1(dhcp-config)#network 192.168.21.0  
255.255.255.0  
  
R1(dhcp-config)#exit
```

Crear un pool de DHCP para la VLAN 23

```
R1(config)#ip dhcp pool ENGNR  
  
R1(dhcp-config)#dns-server 10.10.10.10  
R1(dhcp-config)#domain-name ccna-sa.com  
R1(dhcp-config)#default-router 192.168.23.1  
  
R1(dhcp-config)#network 192.168.23.0  
255.255.255.0  
  
R1(dhcp-config)#exit
```

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

La configuración del R2 incluye las siguientes tareas:

Comandos:

Crear una base de datos local con una cuenta de usuario

```
R2(config)#user webuser privilege 15 secret  
cisco12345
```

Habilitar el servicio del servidor HTTP

No soporta

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

No 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
```

```
R2(config-if)#ip nat inside
```

Configurar la NAT dinámica dentro de una ACL privada

```
R2(config)#access-list 1 permit 192.168.21.0  
0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.23.0  
0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.4.0
0.0.0.255
```

Defina el pool de direcciones IP públicas utilizables.

```
R2(config)#ip nat pool INTERNET
209.165.200.232 209.165.200.237 netmask
255.255.255.248
```

Definir la traducción de NAT dinámica

```
R2(config)#ip nat inside source list 1 pool
INTERNET
```

### 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.

Figura 21. Configuración PC-C

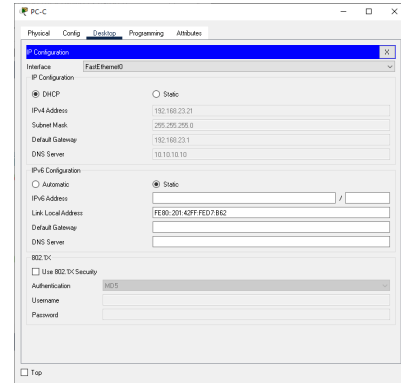


Figura 22. Ping de PC-A a PC-C

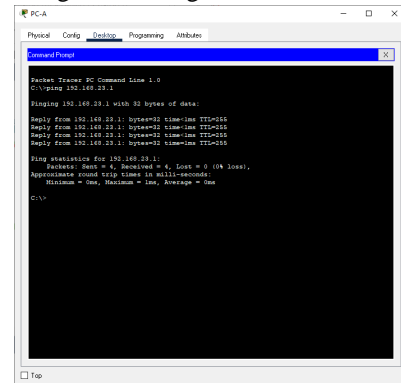
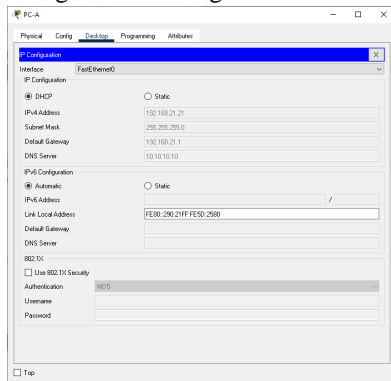


Figura 23. Navegador Web

Figura 20. Configuración PC-A



## Parte 6: Configurar NTP

Tabla 14. Configuración NTP en R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 02:02:50 13 Jul 2021
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	R1(config)#ntp update-calendar

calendario periódicas con hora NTP.	
-------------------------------------	--

Figura 24. Configuración de NTP en R1.

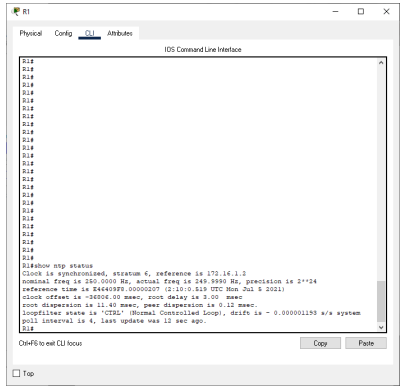
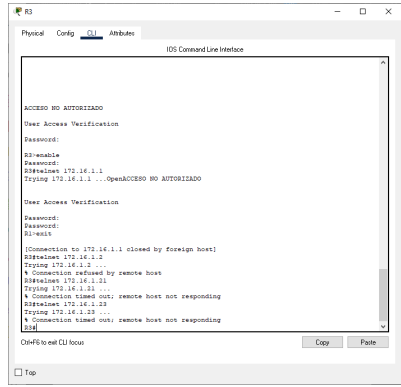


Figura 25. Funcionamiento de la ACL.



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

**Paso 1. Restringir el acceso a las líneas VTY en el R2**

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

R2(config)#ip access-list standard ADMIN-MGT

Aplicar la ACL con nombre a las líneas VTY

Permitir acceso por Telnet a las líneas de VTY

R2(config-std-nacl)#permit host 172.16.1.1

R2(config-std-nacl)#exit

Verificar que la ACL funcione como se espera

R2(config)#line vty 0 4

R2(config-line)#access

R2(config-line)#access-class ADMIN-MGT in

R2(config-line)#exit

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

Tabla 15. Comandos de verificación.

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  <b>Nota:</b> 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

<https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/>.

### RESULTADOS

La configuración que se hizo con el protocolo OSPF genera gran seguridad similar, pero mas simplificado a otros protocolos. Se realizó con el software CISCO Packet Tracer que simulamos la red lo mas parecido a la realiza de un campo laboral.

### BIBLIOGRAFÍA

CISCO Networking Academy. Capitulo 5 Ethernet. Recuperado de: <https://contenthub.netacad.com/legacy/CCNA/ITN/6.0/es/index.html#5.1.1.1>

Definiciones (2020). DNS. Recuperado de: [https://definicion.de/dns/#:~:text=La%20sigla%20DNS%20proviene%20de,Protocolo%20o%20Protocolo%20de%20Internet\).](https://definicion.de/dns/#:~:text=La%20sigla%20DNS%20proviene%20de,Protocolo%20o%20Protocolo%20de%20Internet).)

Redes de computador (2018). Dispositivos enrutadores: Routers. Recuperado de: [http://redesdecomputadores.umh.es/red/routers/default.html#:~:text=El%20router%20\(enrutador%20o%20encaminador,de%20red%20o%20redes%20oenteras.](http://redesdecomputadores.umh.es/red/routers/default.html#:~:text=El%20router%20(enrutador%20o%20encaminador,de%20red%20o%20redes%20oenteras.)

Redes Zone (2019). VLANs: Qué son, tipos y para que sirven. Recuperado de: