

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

JENNY LORENA ROSERO AYALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI  
INGENIERIA ELECTRONICA  
BOGOTA D.C  
2021

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

JENNY LORENA ROSERO AYALA

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

DIRECTOR:

MSc. GERARDO GRANADOS ACUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI  
INGENIERIA ELECTRONICA  
BOGOTA D.C

2020

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Bogotá D.C, noviembre 2021

## **AGRADECIMIENTOS**

A Dios, quien me ha dado su bendición para tener la voluntad y la dedicación de entregar mi esfuerzo y mi tiempo a este proyecto de vida.

A mis padres, hermano y sobrinos quienes han sido mi inspiración durante este tiempo, y a pesar de la distancia siempre me han apoyado e incentivado a cumplir mis proyectos.

A mi esposo quien ha sido parte fundamental de este proyecto, con su apoyo incondicional y quien siempre me ha motivado a llegar a la cima con trabajo y dedicación.

Finalmente, a la universidad y sus docentes quien con este método de educación han facilitado y hecho posible este gran sueño a pesar de los miles de kilómetros de distancia.

## CONTENIDO

AGRADECIMIENTOS .....	4
CONTENIDO .....	5
LISTA DE FIGURAS .....	6
GLOSARIO .....	8
RESUMEN .....	9
ABSTRACT .....	9
INTRODUCCION .....	10
DESARROLLO .....	11
Escenario 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.....	11
Escenario 2: Configurar la capa 2 de la red y el soporte de Host. ....	20
Escenario 3: Configurar los protocolos de enrutamiento .....	32
Escenario 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy) .....	40
Escenario 5: Seguridad .....	51
Escenario 6: Configure las funciones de Administración de Red.....	57
CONCLUSIONES .....	69
BIBLIOGRAFIA .....	70

## LISTA DE FIGURAS

Figura 1 Topología de la Red.....	11
Figura 2 Conf. direccionamiento PC1 .....	19
Figura 3 Conf. direccionamiento PC4 .....	20
Figura 4 Verificación servicios DHCP en PC2 .....	26
Figura 5 Verificación servicios DHCP en PC3 .....	27
Figura 6 Verificación comunicación PC1.....	28
Figura 7 Verificación comunicación PC2.....	29
Figura 8 Verificación comunicación PC3.....	30
Figure 9 Verificación comunicación PC4.....	31
Figure 10 Ejecución Neighbor IPv6 en R2 .....	36
Figure 11 Ejecución Address family IPv4 en R2 .....	37
Figure 12 Ejecución Interfaz Null 0 en R1 .....	38
Figure 13 Ejecución neighbor IPv6 en R1.....	39
Figure 14 Ejecución comando Address family en R1 .....	39
Figure 15 Ejecución IP SLA en D1.....	40
Figure 16 Ejecución IP SLA en switch D2.....	41
Figure 17 Ejecución IP SLA numero de rastreo 4 standby 104 en D1 .....	42
Figure 18 Ejecución IP SLA numero de rastreo 4 standby 114 en D1 .....	43
Figure 19 Ejecución IP SLA numero de rastreo 4 standby 124 en D1 .....	44
Figure 20 Ejecución IP SLA numero de rastreo 6 standby 106 en D1 .....	44
Figure 21 Ejecución IP SLA numero de rastreo 6 standby 106 en D1 .....	45
Figure 22 Ejecución IP SLA numero de rastreo 6 standby 126 en D1 .....	46
Figure 23 Ejecución IP SLA numero de rastreo 4 standby 104 en D2 .....	47
Figure 24 Ejecución IP SLA numero de rastreo 6 standby 116 en D2 .....	48
Figure 25 Ejecución IP SLA numero de rastreo 4 standby 124 en D2 .....	48
Figure 26 Ejecución IP SLA numero de rastreo 6 standby 106 en D2 .....	49
Figure 27 Ejecución IP SLA numero de rastreo 6 standby 116 en D2 .....	50
Figure 28 Ejecución IP SLA numero de rastreo 6 standby 126 en D2 .....	51
Figure 29 Ejecucion Algorithm-type en R3.....	51
Figure 30 Ejecución comando AAA en A1 .....	53
Figure 31 Ejecución comando acct en R1.....	53
Figure 32 Ejecución comando acct en R3.....	54
Figure 33 Ejecución comando Radius Server en D1 .....	54
Figure 34 Ejecución comando Radius Server en D2 .....	55
Figure 35 Ejecución comando Radius Server en A1.....	55
Figure 37 Ejecución nivel Warning en R1. ....	59
Figure 38 Ejecución nivel Warning en R3 .....	59
Figure 39 Ejecución nivel Warning en D1 .....	60
Figure 40 Ejecución nivel Warning en D2 .....	60

Figure 41 Ejecución nivel Warning en A1 .....	61
Figure 42 Ejecución comando contact en R1.....	62
Figure 43 Ejecución comando contact en R3.....	62
Figure 44 Ejecución comando contact en D1.....	63
Figure 45 Ejecución comando contact en D2.....	63
Figure 46 Ejecución comando contact en A1.....	64
Figure 47 Ejecución comando SNMP-NMS en R1.....	64
Figure 48 Ejecución comando SNMP-NMS en R3.....	65
Figure 49 Ejecución comando SNMP-NMS en D1.....	65
Figure 50 Ejecución comando SNMP-NMS en D2.....	66
Figure 51 Ejecución comando SNMP-NMS en A1.....	66
Figure 52 Ejecución comando enable traps,config y ospf en R3,D1 y D2.....	67
Figure 53 Ejecución comando enable traps,config y ospf en R3,D1 y D2.....	67
Figure 54 Ejecución comando enable traps,config y ospf en A1.....	68

## GLOSARIO

### CCNP

Cisco Certified Network Profesional, proporcionan conocimientos avanzados en el diseño de redes de LAN, WAN, grandes redes y redes de conexión telefónica tanto enrutadas como conmutadas.

### Interfaces troncales IEEE 802.1Q

Es un enlace que se configura en uno o mas puertos de un **switch** para permitir el paso del trafico de las distintas VLANs que se ha configurado. El protocolo esencial que da vida al enlace troncal es el que pertenece al estándar IEEE 802.1Q. Esto permite que las tramas Ethernet viajen a través de la red con una etiqueta que contiene el identificador VLAN.

### RSTP

Rapid Spanning Tree Protocol, proviene loops en una red de switches. Este suplanta a su antecesor, el protocolo STP. RSTP trae consigo varias mejoras al respecto a STP principalmente en lo que tiene que ver con tiempos de convergencia.

### LACP

Protocolo de la capa de enlace de datos definido en el estándar IEEE 802.3ad. Proporciona un método para controlar la agrupación de varios puertos físicos y formar un único canal lógico.

### OSPF

Open Shortest Path First es un protocolo usado para distribuir información de enrutamiento dentro de un único sistema autónomo.

### AAA

Authentication, Authorization and Accounting, lo cual permite configurar acceso granular y capacidad de auditoría a un dispositivo IOS.

## **RESUMEN**

Se realizó la configuración de una red con el fin de crear accesibilidad de un punto a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada y para que los protocolos configurados estén operativos. Se realizó un proceso de simulación con una topología de red establecida, el cual se ejecutó mediante el software Cisco Packet Tracer y aunque se intentó simular y hacer las configuraciones en el software de GNS3, los resultados evidencian que existen diferencias entre estos dos programas al momento de ejecutar los comandos. Por lo tanto, se concluye que la utilización de diferentes softwares tiene influencia al momento de ejecutar ciertos comandos tanto en un programa como en el otro.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

The configuration of a network was carried out in order to create accessibility from one point to another, so that the hosts have a reliable support of the default gateway and so that the configured protocols are operational. A simulation process was carried out with an established network topology, which was executed through the Cisco Packet Tracer software and although an attempt was made to simulate and make the configurations in the GNS3 software, the results show that there are differences between these two programs at the moment. executing the commands. Therefore, it is concluded that the use of different software has an influence when executing certain commands both in one program and in the other.

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics.

## INTRODUCCION

Cuando se habla de telecomunicaciones, ingeniería de redes, conexión inalámbrica o Wi-Fi, involucra un ámbito de trabajo y un sector que aún está en desarrollo y del cual se esperan grandes avances. El diplomado en Cisco CCNP supone una gran diferencia y un gran progreso en la vida de todo profesional que trabaje en el entorno de redes, con las infraestructuras de este sector y los servicios o el funcionamiento de los equipos digitales de las empresas, compañías y diferentes grupos.

Es por ello que el trabajo muestra la construcción y la configuración de una topología de red en donde se configuran desde los parámetros más básicos hasta protocolos de enrutamiento y características de administración de red, el cual se dividió en seis escenarios.

La metodología para el desarrollo de este proyecto se basa en la ejecución de la configuración de los comandos necesarios para realizar toda la programación del direccionamiento, los protocolos de enrutamiento, las configuraciones de seguridad y las de administración de red, mediante una simulación en el programa de Packet Tracer de Cisco.

## DESARROLLO

**Escenario 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.**

**Paso 1: Cablear la red como se muestra en la topología.**

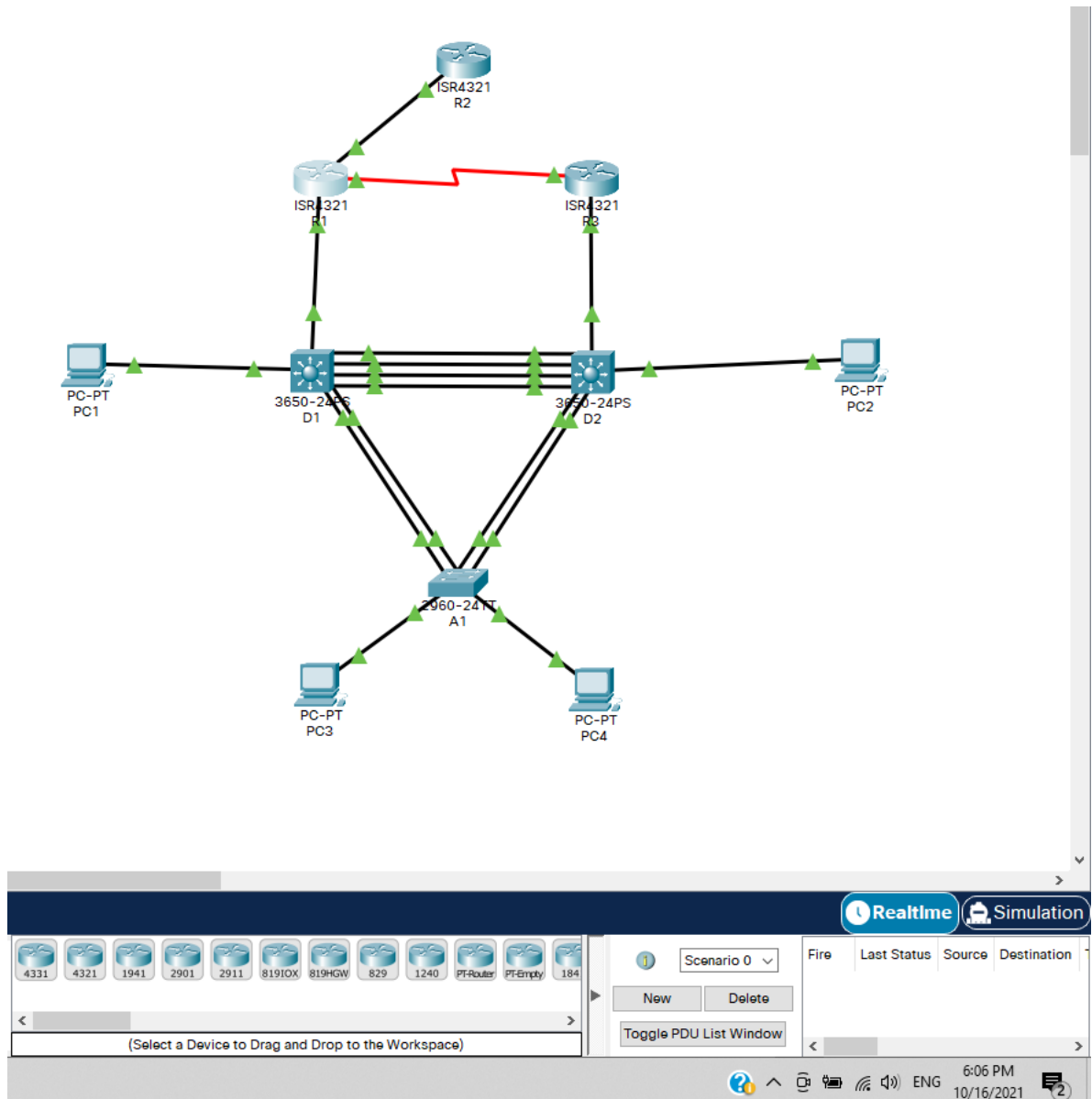


Figura 1 Topología de la Red

## **Paso 2: Configurar los parámetros básicos para cada dispositivo.**

Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación.

### **Router R1**

```
Router>enable
Router#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Router(config)# hostname R1
R1 (config)#ipv6 unicast-routing
R1 (config)#no ip domain lookup
R1 (config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1 (config)#line con 0
R1 (config-line)#exec-timeout 0 0
R1 (config)#logging synchronous
R1 (config)#exit
R1 (config)#interface g0/0/0
R1 (config-if)#ip address 209.165.200.225 255.255.255.224
R1 (config-if)#ipv6 address fe80::1:1 link-local
R1 (config-if)#ipv6 address 2001:db8:200::1/64
R1 (config-if)#no shutdown
```

```
R1 (config-if)#exit
R1 (config)#interface g0/0/1
R1 (config-if)#ip address 10.0.10.1 255.255.255.0
R1 (config-if)#ipv6 address fe80::1:2 link-local
R1 (config-if)#ipv6 address 2001:db8:100:1010::1/64
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface s0/1/0
R1 (config-if)#ip address 10.0.13.1 255.255.255.0
R1 (config-if)#ipv6 address fe80::1:3 link-local
R1 (config-if)#ipv6 address 2001:db8:100:1013::1/64
R1 (config-if)#no shutdown
R1 (config-if)#exit
```

## **Router R2**

```
Router>enable
Router#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Router(config)# hostname R2
R2 (config)#ipv6 unicast-routing
R2 (config)#no ip domain lookup
R2 (config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2 (config)#line con 0
R2 (config-line)#exec-timeout 0 0
R2 (config)#logging synchronous
R2 (config)#exit
R2 (config)#interface g0/0/0
R2 (config-if)#ip address 209.165.200.226 255.255.255.224
R2 (config-if)#ipv6 address fe80::2:1 link-local
R2 (config-if)#ipv6 address 2001:db8:200::2/64
R2 (config-if)#no shutdown
```

```
R2 (config-if)#exit
R2 (config)#interface Loopback 0
R2 (config-if)#ip address 2.2.2.2 255.255.255.255
R2 (config-if)#ipv6 address fe80::2:3 link-local
R2 (config-if)#ipv6 address 2001:db8:2222::1/128
R2 (config-if)#no shutdown
R2 (config-if)#exit
```

### **Router R3**

```
Router>enable
Router#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Router(config)# hostname R3
R3 (config)#ipv6 unicast-routing
R3 (config)#no ip domain lookup
R3 (config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3 (config)#line con 0
R3 (config-line)#exec-timeout 0 0
R3 (config)#logging synchronous
R3 (config)#exit
R3 (config)#interface g0/0/1
R3 (config-if)#ip address 10.0.11.1 255.255.255.0
R3 (config-if)#ipv6 address fe80::3:2 link-local
R3 (config-if)#ipv6 address 2001:db8:100:1011::1/64
R3 (config-if)#no shutdown
```

```
R3 (config-if)#exit
R3 (config)#interface s0/1/0
R3 (config-if)#ip address 10.0.13.3 255.255.255.255
R3 (config-if)#ipv6 address fe80::3:3 link-local
R3 (config-if)#ipv6 address 2001:db8:100:1010::2/64
R3 (config-if)#no shutdown
R3 (config-if)#exit
```

## Switch D1

```
Switch>enable
Switch#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Switch(config)# hostname D1
D1 (config)#ip routing
D1 (config)#ipv6 unicast-routing
D1 (config)#no ip domain lookup
D1 (config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1 (config)#line con 0
D1 (config-line)#exec-timeout 0 0
D1 (config)#logging synchronous
D1 (config)#exit
D1 (config)#vlan 100
D1 (config-vlan)#name Management
D1 (config-vlan)#exit
D1 (config)#vlan 101
D1 (config-vlan)#name UserGroupA
D1 (config-vlan)#exit
D1 (config)#vlan 102
D1 (config-vlan)#name UserGroupB
D1 (config-vlan)#exit
D1 (config)#vlan 999
D1 (config-vlan)#name NATIVE
D1 (config-vlan)#exit
D1 (config)#interface g1/0/11
D1 (config-if)#no switchport
D1 (config-if)#ip address 10.0.10.2 255.255.255.0
D1 (config-if)#ipv6 address fe80::d1:1 link-local
D1 (config-if)#ipv6 address 2001:db8:100:1010::2/64
D1 (config-if)#no shutdown
D1 (config-if)#exit
D1 (config)#interface vlan 100
D1 (config-if)#ip address 10.0.100.1 255.255.255.0
D1 (config-if)#ipv6 address fe80::d1:2 link-local
```

```

D1 (config-if)#ipv6 address 2001:db8:100:100::1/64
D1 (config-if)#no shutdown
D1 (config-if)#exit
D1 (config)#interface vlan 101
D1 (config-if)#ip address 10.0.101.1 255.255.255.0
D1 (config-if)#ipv6 address fe80::d1:3 link-local
D1 (config-if)#ipv6 address 2001:db8:100:101::1/64
D1 (config-if)#no shutdown
D1 (config-if)#exit
D1 (config)#interface vlan 102
D1 (config-if)#ip address 10.0.102.1 255.255.255.0
D1 (config-if)#ipv6 address fe80::d1:4 link-local
D1 (config-if)#ipv6 address 2001:db8:100:102::1/64
D1 (config-if)#no shutdown
D1 (config-if)#exit
D1 (config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1 (config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1 (config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1 (config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1 (config)#ip dhcp pool VLAN-101
D1 (config)#network 10.0.101.0 255.255.255.0
D1 (config)#default-router 10.0.101.254
D1 (config)#exit
D1 (config)#ip dhcp pool VLAN-102
D1 (dhcp-config)#network 10.0.102.0 255.255.255.0
D1 (dhcp-config)#default-router 10.0.102.254
D1 (dhcp-config)#exit
D1 (config-if)#interface range g1/0/7-24
D1 (config-if)#shutdown
D1 (config-if)#exit

```

## Switch D2

```

Switch>enable
Switch#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Switch(config)# hostname D2
D2 (config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2 (config)#line con 0
D2 (config-line)#exec-timeout 0 0
D2 (config-line)#logging synchronous
D2 (config-line)#exit
D2 (config)#vlan 100
D2 (config-vlan)#name Management

```

```
D2 (config-vlan)#exit
D2 (config)#vlan 101
D2 (config-vlan)#name UserGroupA
D2 (config-vlan)#exit
D2 (config)#vlan 102
D2 (config-vlan)#name UserGroupB
D2 (config-vlan)#exit
D2 (config)#vlan 999
D2 (config-vlan)#name NATIVE
D2 (config-vlan)#exit
D2 (config)#interface g1/0/11
D2 (config-if)#no switchport
D2 (config)#ip address 10.0.11.2 255.255.255.0
D2 (config-if)#ipv6 address fe80::d1:1 link-local
D2 (config-if)#ipv6 address 2001:db8:100:1011::2/64
D2 (config-if)#no shutdown
D2 (config-if)#exit
D2 (config)#interface vlan 100
D2 (config-if)#ip address 10.0.100.2 255.255.255.0
D2 (config-if)#ipv6 address fe80::d2:2 link-local
D2 (config-if)#ipv6 address 2001:db8:100:100::2/64
D2 (config-if)#no shutdown
D2 (config-if)#exit
D2 (config)#interface vlan 101
D2 (config-if)#ip address 10.0.101.2 255.255.255.0
D2 (config-if)#ipv6 address fe80::d2:3 link-local
D2 (config-if)#ipv6 address 2001:db8:100:101::2/64
D2 (config-if)#no shutdown
D2 (config-if)#exit
D2 (config)#interface vlan 102
D2 (config-if)#ip address 10.0.102.2 255.255.255.0
D2 (config-if)#ipv6 address fe80::d2:4 link-local
D2 (config-if)#ipv6 address 2001:db8:100:102::2/64
D2 (config-if)#no shutdown
D2 (config-if)#exit
D2 (config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2 (config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2 (config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2 (config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2 (config)#ip dhcp pool VLAN-101
D2 (dchp-config)#network 10.0.101.0 255.255.255.0
D2 (dchp-config)#default-router 10.0.101.254
D2 (dchp-config)#exit
D2 (config)#ip dhcp pool VLAN-102
D2 (dchp-config)#network 10.0.102.0 255.255.255.0
```

```
D2 (dchp-config)#default-router 10.0.102.254
D2 (dchp-config)#exit
D2 (config)#interface range g1/0/7-24
D2 (config)#shutdown
D2 (config)#exit
```

## Switch A1

```
Switch>enable
Switch#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
Switch(config)# hostname A1
A1 (config)#no ip domain lookup
A1 (config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1 (config)#line con 0
A1 (config-line)#exec-timeout 0 0
A1 (config-line)#logging synchronous
A1 (config-line)#exit
A1 (config)#vlan 100
A1 (config-vlan)#name Management
A1 (config-vlan)#exit
A1 (config)#vlan 101
A1 (config-vlan)#name UserGroupA
A1 (config-vlan)#exit
A1 (config)#vlan 102
A1 (config-vlan)#name UserGroupB
A1 (config-vlan)#exit
A1 (config)#vlan 999
A1 (config-vlan)#name NATIVE
A1 (config-vlan)#exit
A1 (config)#interface vlan 100
A1 (config-if)#ip address 10.0.100.3 255.255.255.0
A1 (config-if)#ipv6 address fe80::a1:1 link-local
A1 (config-if)#ipv6 address 2001:db8:100:100::3/64
A1 (config-if)#no shutdown
A1 (config-if)#exit
A1 (config)#interface range f0/5-22
A1 (config)#shutdown
A1 (config)#exit
```

b. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.

Se ingresa el siguiente código en todos los dispositivos **R1, R2, R3, D1, D2, A1**.

### Router R1

```
R1>enable
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

c. Configure el direccionamiento de los host PC1 y PC4 como se muestra en la tabla de direccionamiento.

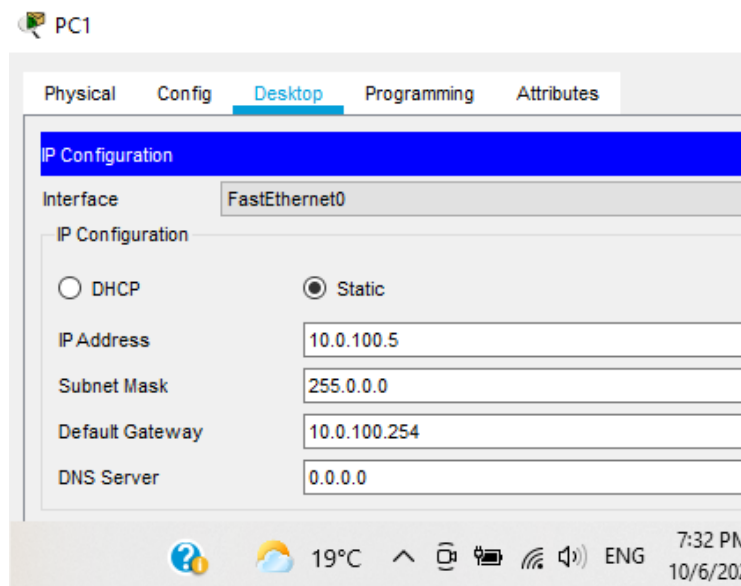


Figura 2 Conf. direccionamiento PC1

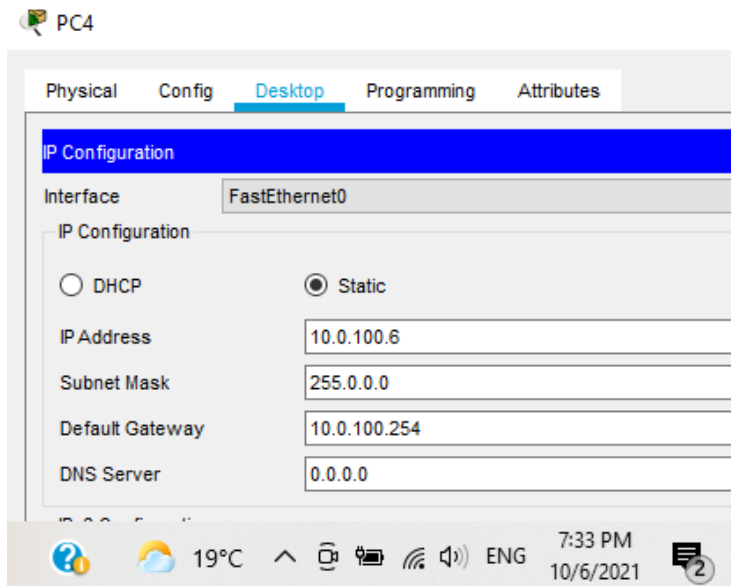


Figura 3 Conf. direccionamiento PC4

## Escenario 2: Configurar la capa 2 de la red y el soporte de Host.

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Para habilitar los enlaces trunk 802.1Q en D1 ingrese el siguiente código

Habilitamos los enlaces trunk 802.1Q entre

### D1 y D2

D1>enable

D1#conf terminal

Enter configuration commands,one per line. End with CNTL/Z

D1(config)#interface range gigabitEthernet 1/0/1-4

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

### D2 y D1

D2>enable

D2#conf terminal

Enter configuration commands,one per line. End with CNTL/Z

D2(config)#interface range gigabitEthernet 1/0/1-4

```
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
```

### **D1 y A1**

```
D1(config)#interface range gigabitEthernet 1/0/5-6
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
```

### **A1 y D1**

```
A1>enable
A1#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
A1(config)#interface range gigabitEthernet 0/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
```

### **D2 y A1**

```
D2>enable
D2#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
D2(config)#interface range gigabitEthernet 1/0/5-6
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
```

### **A1 y D2**

```
A1>enable
A1#conf terminal
Enter configuration commands,one per line. End with CNTL/Z
A1(config)#interface range gigabitEthernet 0/3-4
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
```

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

### **Switch D1**

```
D1(config)#interface range gigabitEthernet 1/0/1-6  
D1(config-if-range)#switchport trunk native vlan 999
```

```
D1(config)#interface range gigabitEthernet 1/0/5-6  
D1(config-if-range)#switchport trunk native vlan 999
```

### **Switch D2**

```
D2(config)#interface range gigabitEthernet 1/0/1-4  
D2(config-if-range)#switchport trunk native vlan 999
```

```
D2(config)#interface range gigabitEthernet 1/0/1-6  
D2(config-if-range)#switchport trunk native vlan 999
```

### **Switch A1**

```
A1(config)#interface range fastEthernet 0/1-4  
A1(config-if-range)#switchport trunk native vlan 999
```

```
A1(config)#interface range fastEthernet 0/3-4  
A1(config-if-range)#switchport trunk native vlan 999
```

### 2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

Para ejecutar esta acción necesitamos el comando `spanning-tree mode rapid-pvst` en modo configuración.

#### **Switch A1**

```
A1(config)#spanning-tree mode rapid-pvst
```

#### **Switch D1**

```
D1(config)#spanning-tree mode rapid-pvst
```

#### **Switch D2**

```
D2(config)#spanning-tree mode rapid-pvst
```

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge)

#### **Switch D1**

```
D1(config)#spanning-tree vlan 101 root secondary  
D1(config)#spanning-tree vlan 100 root primary  
D1(config)#spanning-tree vlan 102 root primary
```

#### **Switch D2**

```
D1(config)#spanning-tree vlan 100 root secondary  
D1(config)#spanning-tree vlan 101 root primary  
D1(config)#spanning-tree vlan 102 root secondary
```

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

Use los siguientes números de canales:

### **D1 a D2 - Port channel 12**

```
D1(config)#interface range gigabitEthernet 1/0/1-4
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#interface port-channel 12
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)# switchport mode trunk
```

```
D2(config)#interface range gigabitEthernet 1/0/1-4
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)# interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)# switchport mode trunk
```

### **D1 a A1 – Port channel 1**

```
D1(config)#interface range gigabitEthernet 1/0/5-6
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#interface port-channel 1
D1(config-if)# switchport trunk encapsulation dot1q
D1(config-if)# switchport mode trunk
```

### **D2 a A1 – Port channel 2**

```
D2(config)#interface range gigabitEthernet 1/0/5-6
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)# interface port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)# switchport mode trunk
```

**2.6** En todos los switches, configure los puertos de acceso del host (host Access port) que se conectan a PC1, PC2, PC3 y PC4.

Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.

Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

### **Switch D1**

```
D1(config)#interface gigabitEthernet 1/0/23
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)# no shutdown
```

### **Switch D2**

```
D2(config)#interface gigabitEthernet 1/0/23
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)# no shutdown
```

### **Switch A1**

```
A1(config)#interface range fastEthernet 0/23
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)# no shutdown
```

```
A1(config)#interface range fastEthernet 0/24
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)# no shutdown
```

2.7 Verifique los servicios DHCP IPv4. PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 validas.

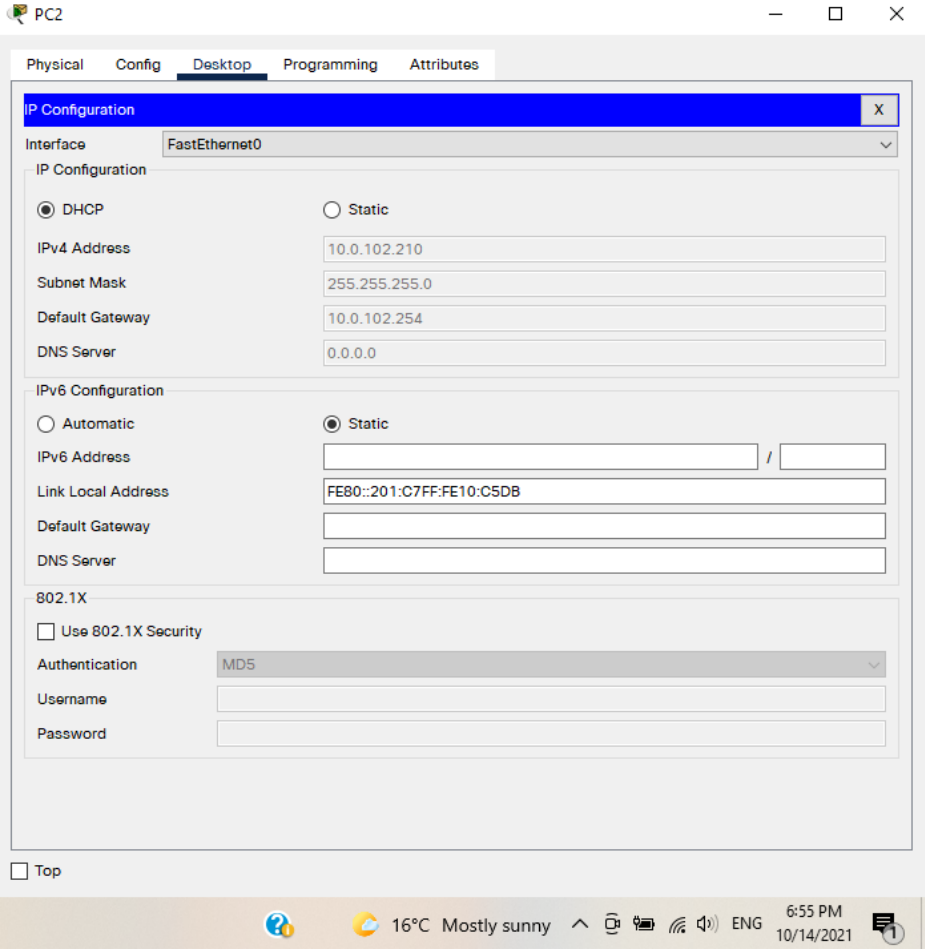


Figura 4 Verificación servicios DHCP en PC2

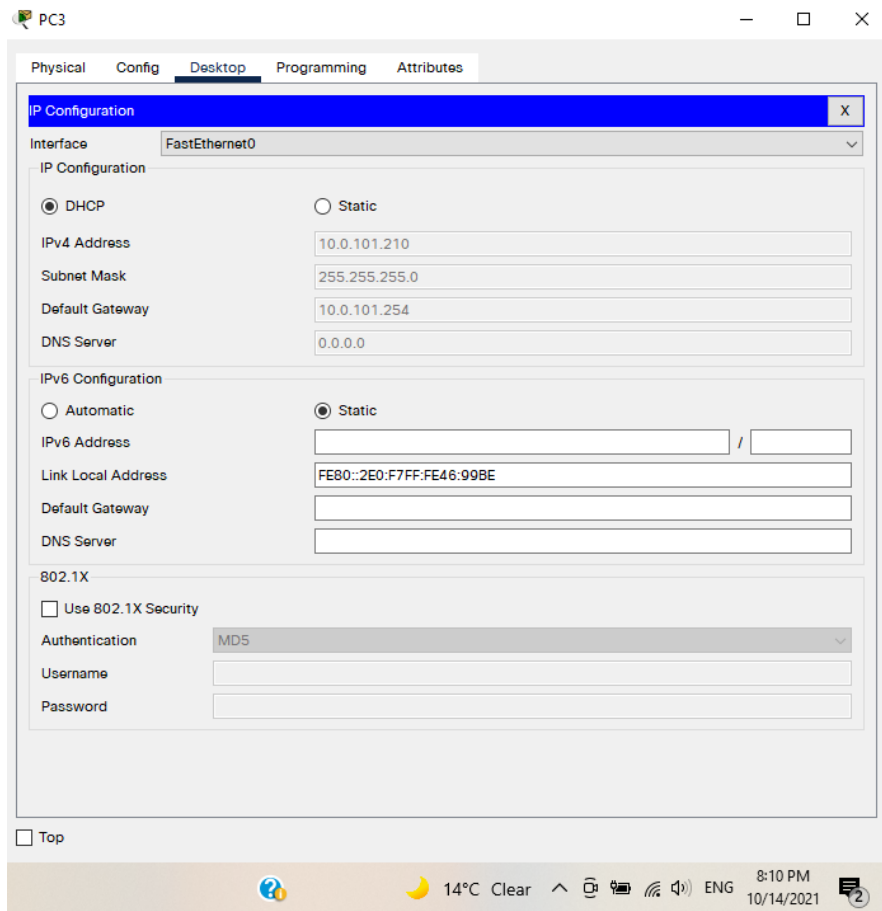
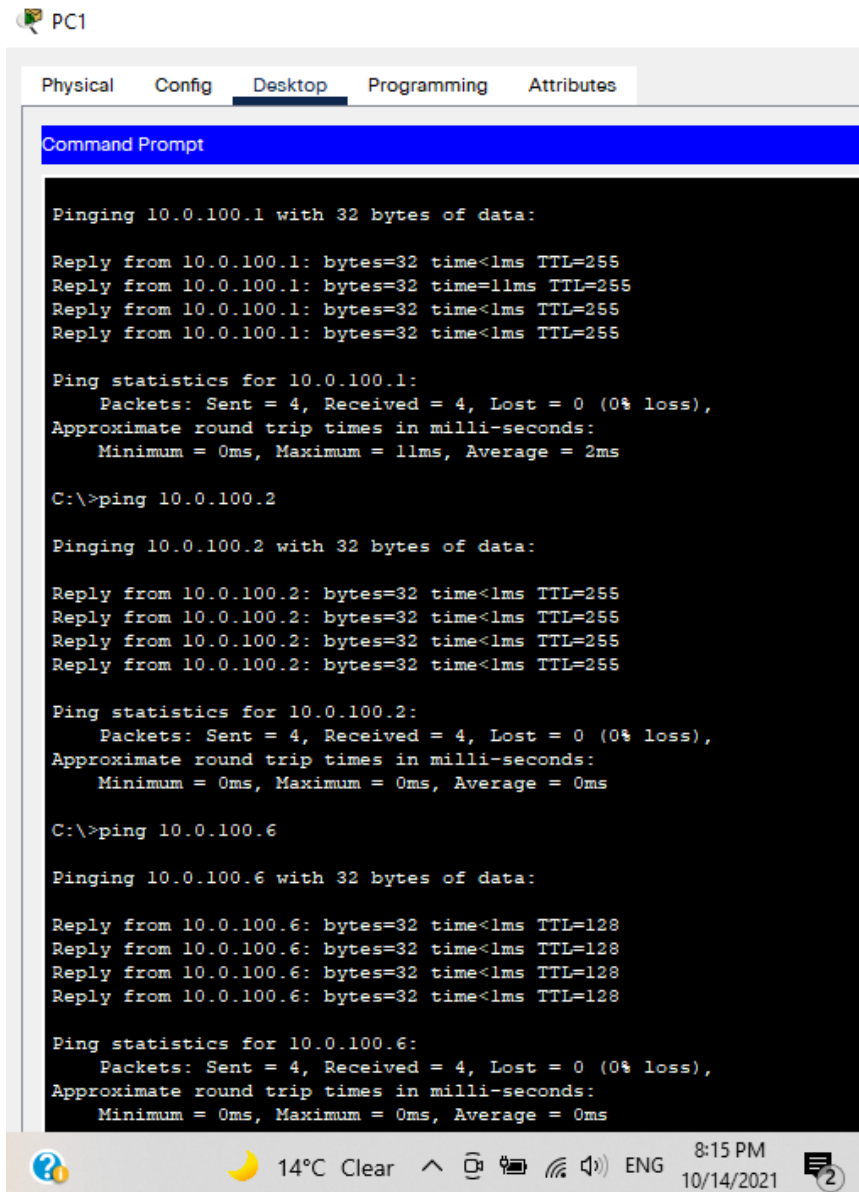


Figura 5 Verificación servicios DHCP en PC3

## 2.8 Verifique la conectividad de la LAN local

PC1 debe hacer ping con:

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC4: 10.0.100.6



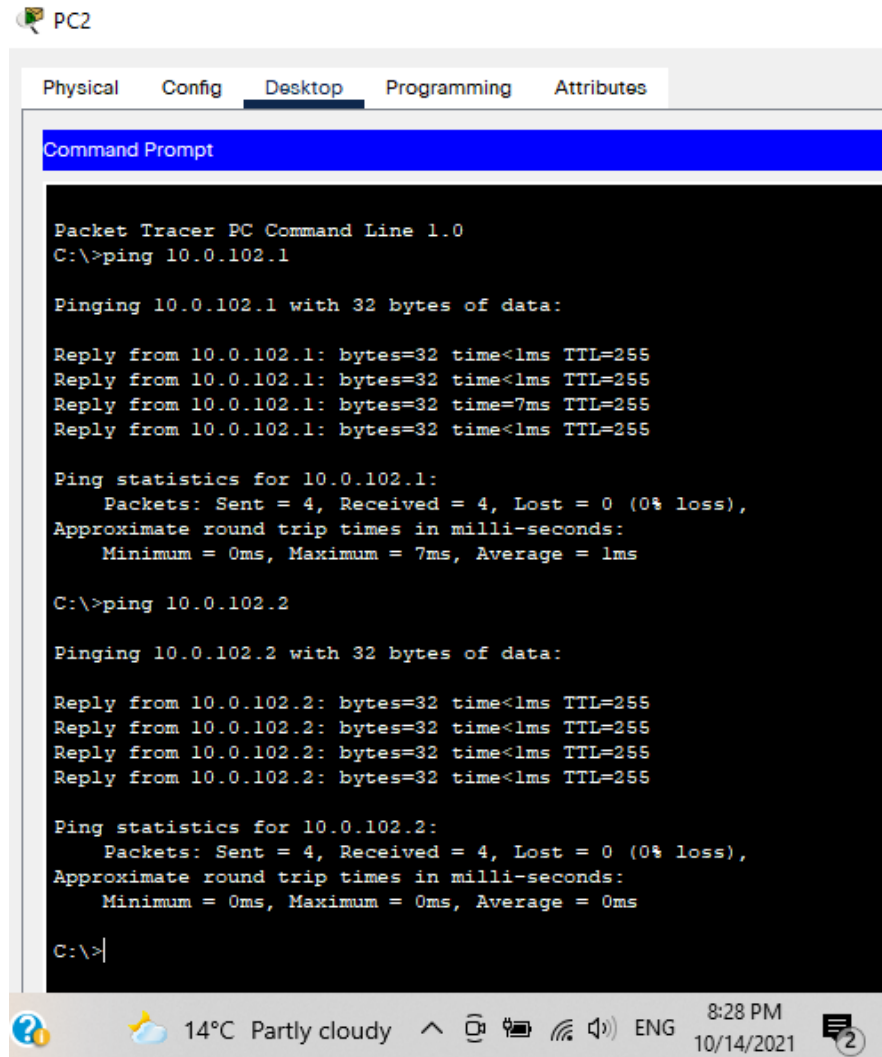
The screenshot shows the Desktop tab of a PC configuration window. A Command Prompt window is open, displaying the results of three ping commands. The first command is for 10.0.100.1, showing four successful replies with 32 bytes of data, a time of <1ms, and a TTL of 255. The second command is for 10.0.100.2, also showing four successful replies with 32 bytes of data, a time of <1ms, and a TTL of 255. The third command is for 10.0.100.6, showing four successful replies with 32 bytes of data, a time of <1ms, and a TTL of 128. The system tray at the bottom shows the date and time as 8:15 PM on 10/14/2021.

```
PC1  
Physical Config Desktop Programming Attributes  
Command Prompt  
Pinging 10.0.100.1 with 32 bytes of data:  
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255  
Reply from 10.0.100.1: bytes=32 time=11ms TTL=255  
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255  
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255  
Ping statistics for 10.0.100.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 11ms, Average = 2ms  
C:\>ping 10.0.100.2  
Pinging 10.0.100.2 with 32 bytes of data:  
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255  
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255  
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255  
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255  
Ping statistics for 10.0.100.2:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms  
C:\>ping 10.0.100.6  
Pinging 10.0.100.6 with 32 bytes of data:  
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128  
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128  
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128  
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128  
Ping statistics for 10.0.100.6:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 6 Verificación comunicación PC1

PC2 debe hacer ping con:

- D1: 10.0.102.1
- D2: 10.0.102.2



The image shows a screenshot of a PC2 interface with a Command Prompt window open. The window title is "Command Prompt" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.102.1

Pinging 10.0.102.1 with 32 bytes of data:

Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time=7ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>ping 10.0.102.2

Pinging 10.0.102.2 with 32 bytes of data:

Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

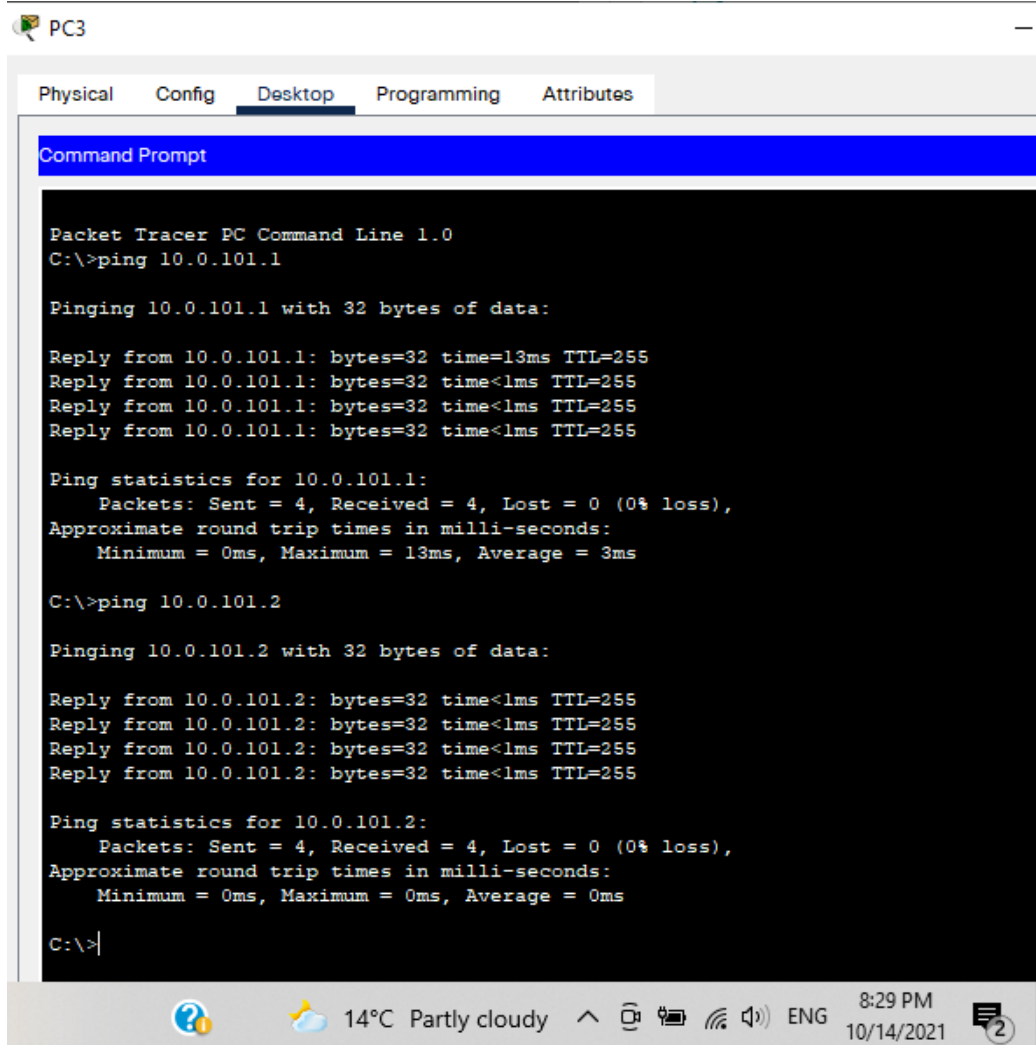
C:\>
```

The taskbar at the bottom shows the system tray with a weather icon (14°C Partly cloudy), network and volume icons, and the system clock (8:28 PM, 10/14/2021).

Figura 7 Verificación comunicación PC2

## PC3

- D1: 10.0.101.1
- D2: 10.0.101.2



The screenshot shows a Windows-style desktop environment for PC3. The 'Desktop' tab is active in the top navigation bar. A Command Prompt window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.101.1

Pinging 10.0.101.1 with 32 bytes of data:

Reply from 10.0.101.1: bytes=32 time=13ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.101.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>ping 10.0.101.2

Pinging 10.0.101.2 with 32 bytes of data:

Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.101.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

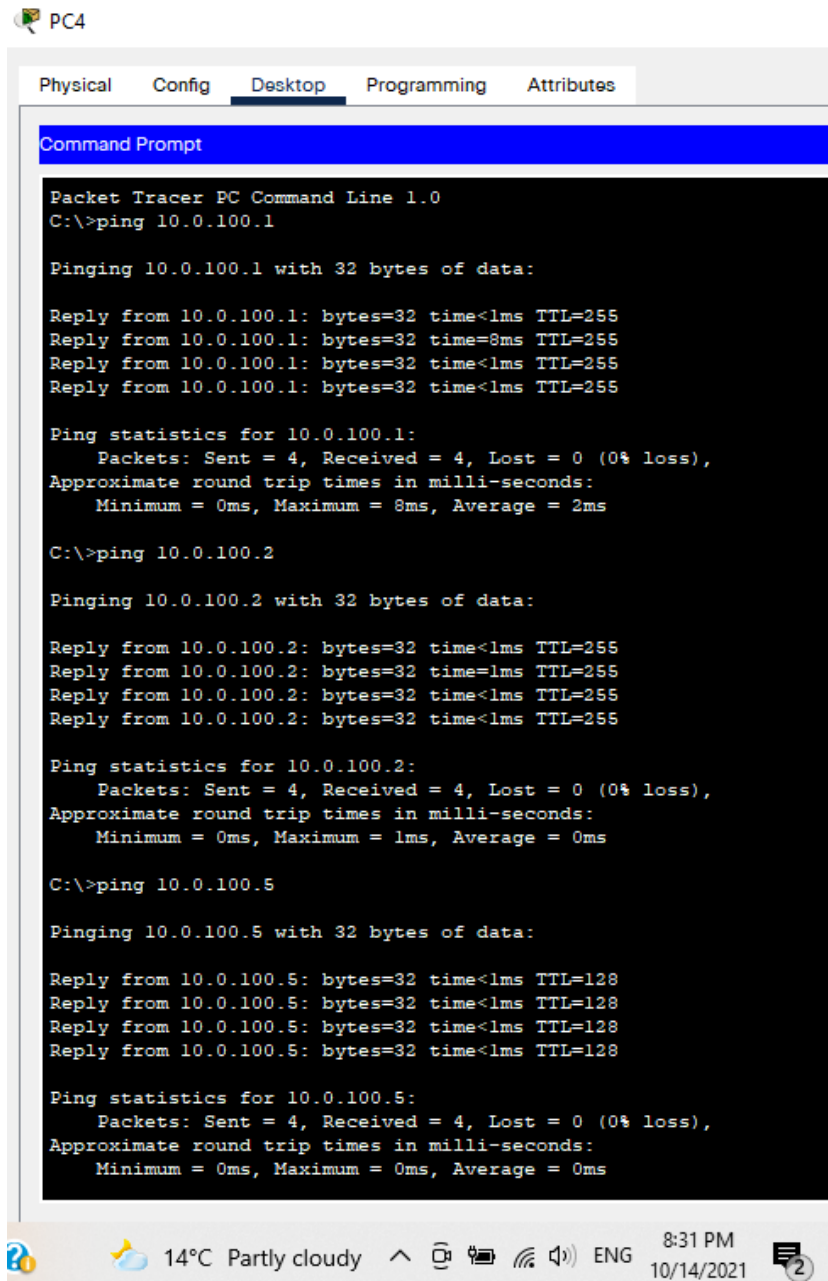
C:\>
```

The taskbar at the bottom shows system icons for help, weather (14°C Partly cloudy), network, volume, and language (ENG). The system clock displays 8:29 PM on 10/14/2021.

Figura 8 Verificación comunicación PC3

## PC4

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC1: 10.0.100.5



The screenshot shows the Desktop tab of a Packet Tracer PC configuration window for PC4. A Command Prompt window is open, displaying the results of three ping commands. The first command is for 10.0.100.1, showing four successful replies with 32 bytes of data, a TTL of 255, and round trip times of 0ms, 8ms, 1ms, and 1ms. The second command is for 10.0.100.2, also showing four successful replies with 32 bytes of data, a TTL of 255, and round trip times of 0ms, 1ms, 1ms, and 1ms. The third command is for 10.0.100.5, showing four successful replies with 32 bytes of data, a TTL of 128, and round trip times of 1ms, 1ms, 1ms, and 1ms. The system tray at the bottom shows the time as 8:31 PM on 10/14/2021, the temperature as 14°C, and the weather as Partly cloudy.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.100.1

Pinging 10.0.100.1 with 32 bytes of data:

Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time=8ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>ping 10.0.100.2

Pinging 10.0.100.2 with 32 bytes of data:

Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time=1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.100.5

Pinging 10.0.100.5 with 32 bytes of data:

Reply from 10.0.100.5: bytes=32 time<1ms TTL=128
Reply from 10.0.100.5: bytes=32 time<1ms TTL=128
Reply from 10.0.100.5: bytes=32 time<1ms TTL=128
Reply from 10.0.100.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 9 Verificación comunicación PC4

### **Escenario 3: Configurar los protocolos de enrutamiento**

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1 y D2), configure single-área OSPFv2 en área 0.

- Use OSPF Process ID 4 y asigne los siguientes router IDs:

R1: 0.0.4.1  
R3:0.0.04.3  
D1:0.0.4.131  
D2:0.0.4.132

#### **Router R1**

```
R1 (config)#router OSPF 4  
R1 (config-router)#router-id 0.0.4.1
```

#### **Router R3**

```
R1 (config)#router OSPF 4  
R1 (config-router)#router-id 0.0.4.3
```

#### **Switch D1**

```
D1 (config)#router OSPF 4  
D1 (config-router)#router-id 0.0.4.131
```

#### **Switch D2**

```
D2 (config)#router OSPF 4  
D2 (config-router)#router-id 0.0.4.132
```

- En R1, R3, D1 y D2 anuncie todas las redes directamente conectadas / VLANs en Área 0.

En R1, no publique la red R1-R2.

En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

- Deshabilite las publicaciones OSPFv2 en:

D1: todas las interfaces excepto G1/0/11  
D2: todas las interfaces excepto G1/0/11.

### Switch D1

```
D1 (config-router)#network 10.0.100.0 0.0.0.255 area 0
```

**Identifica la red y la Wildcard mask**

```
D1 (config-router)# network 10.0.10.0 0.0.0.255 area 0
```

```
D1 (config-router)# network 10.0.101.0 0.0.0.255 area 0
```

```
D1 (config-router)# network 10.0.102.0 0.0.0.255 area 0
```

### Switch D2

```
D2 (config-router)#network 10.0.100.0 0.0.0.255 area 0
```

```
D2 (config-router)# network 10.0.11.0 0.0.0.255 area 0
```

```
D2 (config-router)#network 10.0.101.0 0.0.0.255 area 0
```

```
D2 (config-router)#network 10.0.102.0 0.0.0.255 area 0
```

### Router R1

```
R1 (config-router)#network 10.0.10.0 0.0.0.255 area 0
```

```
R1 (config-router)#network 10.0.13.0 0.0.0.255 area 0
```

```
R1 (config-router)#network 209.165.200.0 0.0.0.255 area 0
```

### Router R3

```
R3 (config-router)#network 10.0.11.0 0.0.0.255 area 0
```

```
R3 (config-router)#network 10.0.13.0 0.0.0.255 area 0
```

**3.2** En la 'Red de la Compañía' (es decir R1,R3,D1 y D2), configure classic single-area OSPFv3 en area 0.

- Use OSPF Process ID 6 y asigne los siguientes router IDs.

R1: 0.0.6.1

R3: 0.0.6.3

D1:0.0.6.131

D2:0.0.6.132

- En R1, R3,D1 y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

- En R1, no publique la red R1-R2
- En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.
- Deshabilite las publicaciones OSPFv3 en:

D1: todas las interfaces excepto G1/0/11

D2: todas las interfaces excepto G1/0/11

### Router R1

```
R1 (config)# ipv6 router ospf 6           Ejecutar OSPF Process
R1 (config-rtr)# router-id 0.0.6.1      Asignación de los router ID's.
R1 (config-rtr)# default-information originate
R1 (config-rtr)# exit
R1 (config)# interface g0/0/1
R1 (config-if)#ipv6 ospf 6 area 0       Configuración de classic single- area
                                           OSPFv3 en area 0

R1 (config-if)#exit
R1 (config)# interface g0/0/1
R1 (config)# interaface s0/1/0
R1 (config-if)# ipv6 ospf 6 area 0
R1 (config-if)#exit
```

### Router R3

```
R3 (config)# ipv6 router ospf 6
R3 (config-rtr)# router-id 0.0.6.3
R3 (config-if)#exit
R3 (config)# interface g0/0/1
R3 (config-if)# ipv6 ospf 6 area 0
R3 (config-if)#exit
R3 (config)# interface s0/1/0
R3 (config-if)# ipv6 ospf 6 area 0
R3 (config-if)#exit
```

## Switch D1

```
D1 (config)# ipv6 router ospf 6
D1 (config-rtr)# router-id 0.0.6.131
D1 (config-rtr)#exit
D1 (config)#interface g1/0/11
D1 (config-if)# ipv6 ospf 6 area 0
D1 (config-if)# exit
D1 (config)#interface vlan 100
D1 (config-if)# ipv6 ospf 6 area 0
D1 (config-if)# exit
D1 (config)#interface vlan 101
D1 (config-if)# ipv6 ospf 6 area 0
D1 (config-if)# exit
D1 (config)#interface vlan 102
D1 (config-if)# ipv6 ospf 6 area 0
D1 (config-if)# exit
```

## Switch D2

```
D2 (config)# ipv6 router ospf 6
D2 (config-rtr)# router-id 0.0.6.132
D2 (config-rtr)#exit
D2 (config)#interface g1/0/11
D2 (config-if)# ipv6 ospf 6 area 0
D2 (config-if)#exit
D2 (config)#interface vlan 100
D2 (config-if)# ipv6 ospf 6 area 0
D2 (config-if)#exit
D2 (config)#interface vlan 101
D2 (config-if)# ipv6 ospf 6 area 0
D2 (config-if)#exit
```

### 3.3 En R2 en la Red ISP, configure MP-BGP

- Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

## Router R2

R2 (config-router) # ip route 0.0.0.0.0.0.0.0 Loopback0

- Una ruta estatica predeterminada IPv4.
- Una ruta estatica predeterminada IPv6.

## Router R2

R2(config) # ipv6 route ::/0 Loopback0

- Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2

## Router R2

R2 (config)# router bgp 500

R2 (config-router)# bgp router-id 2.2.2.2

- Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

```
R2(config)#
R2(config)#router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# bgp log-neighbor-changes
R2(config-router)# neighbor 2001:DB8:200::1 remote-as 300
^
% Invalid input detected at '^' marker.
R2(config-router)# neighbor 209.165.200.225 remote-as 300
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

11°C Cloudy 11:36 PM 10/15/2021

Figure 10 Ejecución Neighbor IPv6 en R2

**Explicación:** Al momento de configurar y habilitar la relación de vecino IPv6, la dirección IP no es reconocida.

- En IPv4 address family, anuncie:

La red Loopback 0 IPv4 (/32)  
La ruta por defecto (0.0.0/0)

- En IPv6 address family, anuncie:

La red Loopback 0 IPv4 (/128)  
La ruta por defecto (::/0)

```
R2(config-router)#address-family ipv4
^
% Invalid input detected at '^' marker.

R2(config-router)#?
  bgp          BGP specific commands
  distance     Define an administrative distance
  exit         Exit from routing protocol configuration mode
  neighbor     Specify a neighbor router
  network      Specify a network to announce via BGP
  no           Negate a command or set its defaults
  redistribute Redistribute information from another routing protocol
  synchronization Perform IGP synchronization
  timers       Adjust routing timers
R2(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

8:44 PM 11/24/2021

Figure 11 Ejecución Address family IPv4 en R2

**Explicación:** El comando address-family no está disponible en la lista (usado para anunciar la red loopback y la ruta por defecto)

### 3.4 En R1 en la Red ISP, configure MP-BGP.

- Configure dos rutas resumen estáticas a la interfaz Null 0
- Una ruta resumen IPv4 para 10.0.0.0/8

#### Router R1

R1 (config)# 10.0.0.0 255.0.0.0 null0

- Una ruta resumen IPv6 para 2001:db8:100::/48

```

R1(config)#
R1(config)#
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route 2001:db8:100::/48 null0
^
% Invalid input detected at '^' marker.

R1(config)#ipv6 route 2001:db8:100::/48 ?
Dialer          Dialer interface
Ethernet        IEEE 802.3
FastEthernet    FastEthernet IEEE 802.3
GigabitEthernet GigabitEthernet IEEE 802.3z
Loopback        Loopback interface
Serial          Serial
Vlan            Catalyst Vlans
X:X:X:X:X      IPv6 address of next-hop
R1(config)#ipv6 route 2001:db8:100::/48 null
R1(config)#ipv6 route 2001:db8:100::/48 null0

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

11°C Cloudy 10/15/2021 11:52 PM

Figure 12 Ejecución Interfaz Null 0 en R1

**Explicación:** La opción null0 no esta disponible en la lista.

- Configure R1 en BGP ASN 300 y use el route-id 1.1.1.1

### Router R1

```

R1 (config)# router bgp 300
R1 (config-router)# bgp router-id 1.1.1.1

```

- Configure una relación de vecino IPv4 e IPV6 con R2 en ASN 500

### Router R1

```

R1 (config)# router bgp 300
R1 (config-router)# neighbor 209.165.200.226 remote-as 500

```

**IPv4**

```
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
^
% Invalid input detected at '^' marker.
R1(config-router)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:13 PM 11/24/2021

Figure 13 Ejecución neighbor IPv6 en R1

**Explicación:** El direccionamiento IPv6 no se identifica.

- En IPv4 address family:  
Deshabilite la relación de vecino IPv6.  
Habilite la relación de vecino IPv4.  
Anuncie la red 10.0.0.0/8

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.  
Habilite la relación de vecino IPv6.  
Anuncie la red 2001:db8:100::/48

```
R1(config-router)#address-family ipv4 unicast
^
% Invalid input detected at '^' marker.
R1(config-router)#address-family?
% Unrecognized command
R1(config-router)#address-family
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:18 PM 11/24/2021

Figure 14 Ejecución comando Address family en R1

**Explicación:** El comando *address-family* no se encuentra en la lista de comandos para ejecutar.

## Escenario 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1

- Cree dos IP SLAs
  - Use la SLA numero 4 para IPv4.
  - Use la SLA numero 6 para IPv6.

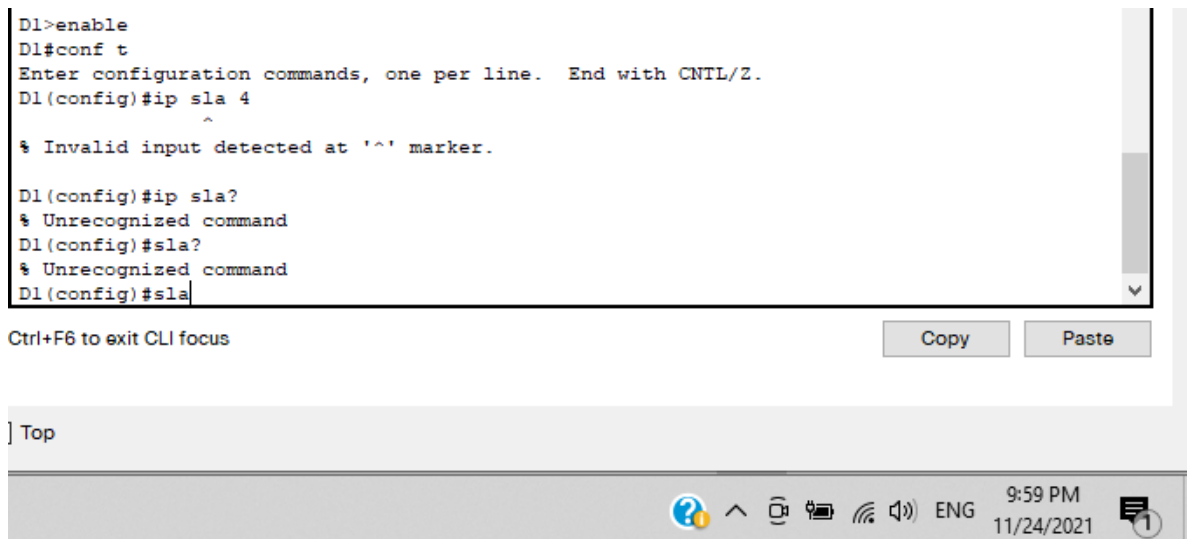
Las IP SLAs prueban la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

Programa la SLA para una implementación inmediata sin tiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

- Use el numero de rastreo 4 para la IP SLA 4.
- Use el numero de rastreo 6 para la IP SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.



```
D1>enable
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla 4
^
% Invalid input detected at '^' marker.

D1(config)#ip sla?
% Unrecognized command
D1(config)#sla?
% Unrecognized command
D1(config)#sla
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:59 PM 11/24/2021

Figure 15 Ejecución IP SLA en D1

**Explicación:** El comando *ip sla* no se encuentra disponible en la lista de comandos, la configuración no se puede llevar a cabo.

#### 4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1

- Cree IP SLAs.
  - Use la SLA numero 4 para IPv4.
  - Use la SLA numero 6 para IPv6.

Las IP SLAs probaran la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.

Programa la SLA para una implementación inmediata sin tiempo de finalización.

- Cree una IP SLA objeto para la IP SLA 4 y una para IP SLA 6.
  - Use el numero de rastreo 4 para la IP SLA 4.
  - Use el numero de rastreo 6 para la SLA 6.

Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

```
D2>enable
D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ip sla
^
% Invalid input detected at '^' marker.
D2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

11:08 PM 11/24/2021

Figure 16 Ejecución IP SLA en switch D2

**Explicación:** El comando *ip sla* no se encuentra disponible en la lista de comandos, la configuración no se puede llevar a cabo.

#### 4.3 En D1 configure HSRPv2

D1 es el router primario para las VLANs 100 y 102, por lo tanto, su prioridad también se cambiará a 150.

Configure HSRP version 2.

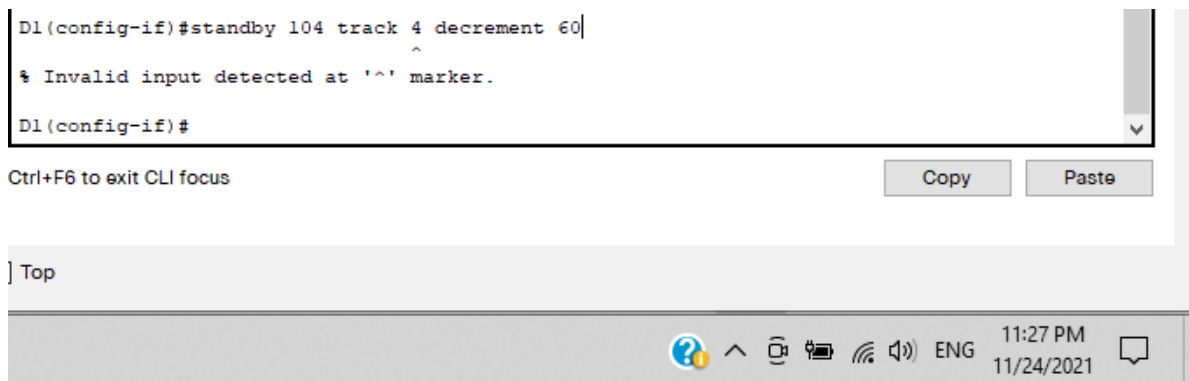
Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).

## Switch D1

```
D1 (config)# interface vlan 100
D1 (config-if)# standby version 2
D1 (config-if)# standby 104 ip 10.0.100.254
%HSRP-6-STATECHANGE: Vlan 100 Grp 104 state Init -> Init
D1 (config-if)#standby 104 priority 150
D1 (config-if)#standby 104 preempt
%HSRP-6-STATECHANGE: Vlan100 Grp 104 state Speak -> Standby.
%HSRP-6-STATECHANGE: Vlan 100 Grp 104 state Standby -> Active.
```

- Rastree el objeto 4 y decremente en 60.



```
D1(config-if)#standby 104 track 4 decrement 60
^
% Invalid input detected at '^' marker.
D1(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

ENG 11:27 PM 11/24/2021

Figure 17 Ejecución IP SLA numero de rastreo 4 standby 104 en D1

**Explicación:** Debido a que no se logro crear las IP SLAs el numero de rastreo no esta configurado y en esta instrucción no se puede continuar.

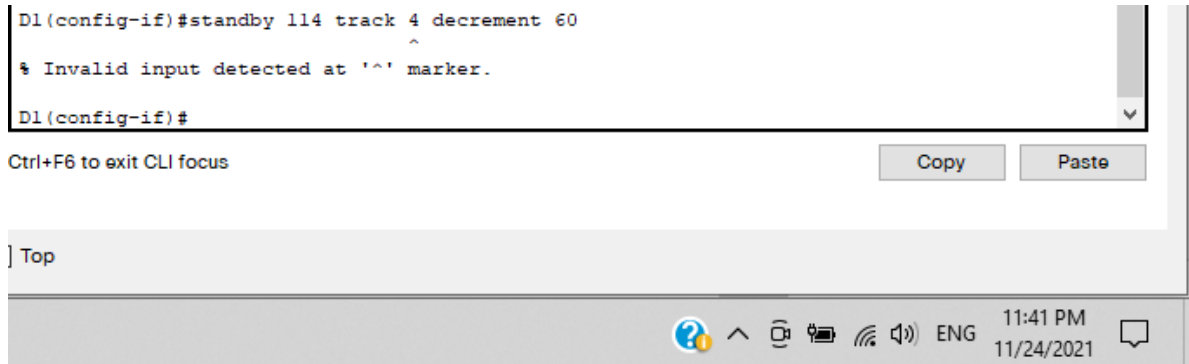
Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

## Switch D1

```
D1 (config)# interface vlan 101
D1 (config-if)# standby version 2
D1 (config-if)# standby 114 ip 10.0.101.254
%HSRP-6-STATECHANGE: Vlan 101 Grp 114 state Init -> Init
D1 (config-if)#standby 114 preempt
```

%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby.  
%HSRP-6-STATECHANGE: Vlan 101 Grp 104 state Standby -> Active.



```
D1(config-if)#standby 114 track 4 decrement 60
^
% Invalid input detected at '^' marker.
D1(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

11:41 PM 11/24/2021

Figure 18 Ejecución IP SLA numero de rastreo 4 standby 114 en D1

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption)
- Rastree el objeto 4 para disminuir en 60.

### Switch D1

```
D1 (config)# interface vlan 102
D1 (config-if)# standby version 2
D1 (config-if)# standby 124 ip 10.0.102.254
%HSRP-6-STATECHANGE: Vlan 102 Grp 124 state Init -> Init
D1 (config-if)#standby 124 priority 150
D1 (config-if)#standby 124 preempt
%HSRP-6-STATECHANGE: Vlan102 Grp 124 state Speak -> Standby.
%HSRP-6-STATECHANGE: Vlan 102 Grp 124 state Standby -> Active.
```

```
D1(config-if)#standby 124 track 4 decrement 60
^
% Invalid input detected at '^' marker.
D1(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

ENG 11:51 PM 11/24/2021

Figure 19 Ejecución IP SLA numero de rastreo 4 standby 124 en D1

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure Ipv6 HSRP grupo 106 para la VLAN 100

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 y decremente en 60.

### Switch D1

```
D1 (config)# interface vlan 100
D1 (config-if)# standby 106 ipv6 autoconfig
D1 (config-if)#standby 106 priority 150
D1 (config-if)#standby 106 preempt
%HSRP-6-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby.
%HSRP-6-STATECHANGE: Vlan 100 Grp 106 state Standby -> Active.
```

```
D1(config-if)#standby track 6 decrement 60
^
% Invalid input detected at '^' marker.
D1(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

ENG 12:05 AM 11/25/2021

Figure 10 Ejecución IP SLA numero de rastreo 6 standby 106 en D1

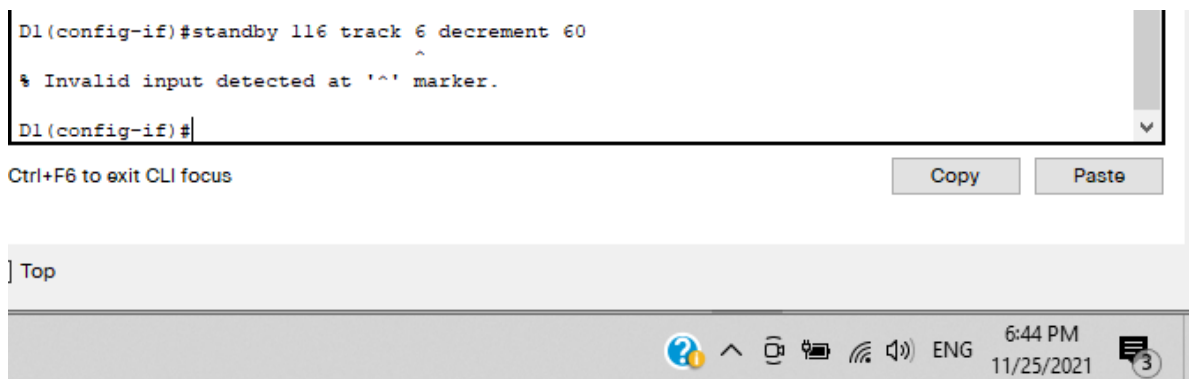
**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure Ipv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando **ipv6 autoconfig**.
- Habilite la preferencia (preemption)
- Registre el objeto 6 y decremente en 60.

### Switch D1

```
D1 (config)# interface vlan 101
D1 (config-if)# standby 116 ipv6 autoconfig
D1 (config-if)#standby 116 preempt
%HSRP-6-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby.
%HSRP-6-STATECHANGE: Vlan 101 Grp 116 state Standby -> Active.
```



```
D1(config-if)#standby 116 track 6 decrement 60
^
% Invalid input detected at '^' marker.
D1(config-if)#
```

Figure 11 Ejecución IP SLA numero de rastreo 6 standby 106 en D1

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando **ipv6 autoconfig**.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 y decremente en 60.

### Switch D1

```
D1 (config)# interface vlan 102
```

```
D1 (config-if)# standby 126 ipv6 autoconfig
D1 (config-if)#standby 126 priority 150
%HSRP-6-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby.
%HSRP-6-STATECHANGE: Vlan 102 Grp 126 state Standby -> Active.

D1 (config-if)# standby 126 preempt
```

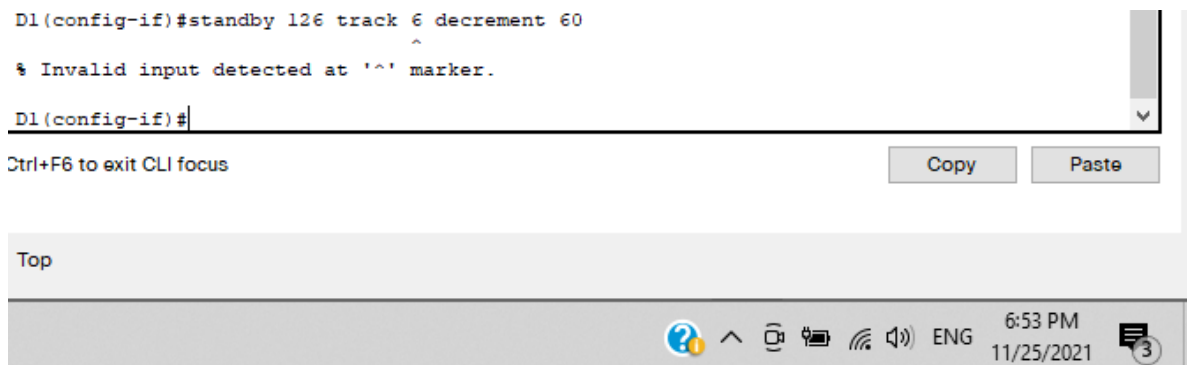


Figure 12 Ejecución IP SLA numero de rastreo 6 standby 126 en D1

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

4.4 En D2, configure HSRP v2.

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.

Configure HSRP versión 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

## Switch D2

```
D2 (config)# interface vlan 100
D2 (config-if)# standby version 2
D2 (config-if)#standby 104 ip 10.0.100.254
%HSRP-6-STATECHANGE: Vlan100 Grp 104 state Init -> Init.
%HSRP-6-STATECHANGE: Vlan 100 Grp 104 state Speak -> Standby.

D2 (config-if)# standby 104 preempt
```

```
D2(config-if)#standby 104 track 4 decrement 60
^
% Invalid input detected at '^' marker.

D2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

7:25 PM 11/25/2021

Figure 13 Ejecución IP SLA numero de rastreo 4 standby 104 en D2

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

## Switch D2

```
D2 (config)# interface vlan 101
D2 (config-if)# standby version 2
D2 (config-if)#standby 114 ip 10.0.101.254
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Init -> Init.
%HSRP-6-STATECHANGE: Vlan 101 Grp 114 state Speak -> Standby.

D2 (config-if)# standby 114 priority 150
D2 (config-if)# standby 114 preempt
%HSRP-6-STATECHANGE: Vlan 101 Grp 114 state Standby -> Active.
```

```
D2(config-if)#standby 116 track 6 decrement 60
^
% Invalid input detected at '^' marker.

D2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

8:42 PM 11/25/2021

Figure 14 Ejecución IP SLA numero de rastreo 6 standby 116 en D2

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

### Switch D2

```
D2 (config)# interface vlan 102
D2 (config-if)# standby version 2
D2 (config-if)#standby 124 ip 10.0.102.254
%HSRP-6-STATECHANGE: Vlan102 Grp 124 state Init -> Init.
%HSRP-6-STATECHANGE: Vlan 102 Grp 124 state Speak -> Standby.

D2 (config-if)# standby 124 preempt
```

```
D2 (config-if)#standby track 4 decrement 60
^
% Invalid input detected at '^' marker.

D2 (config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

8:52 PM 11/25/2021

Figure 15 Ejecución IP SLA numero de rastreo 4 standby 124 en D2

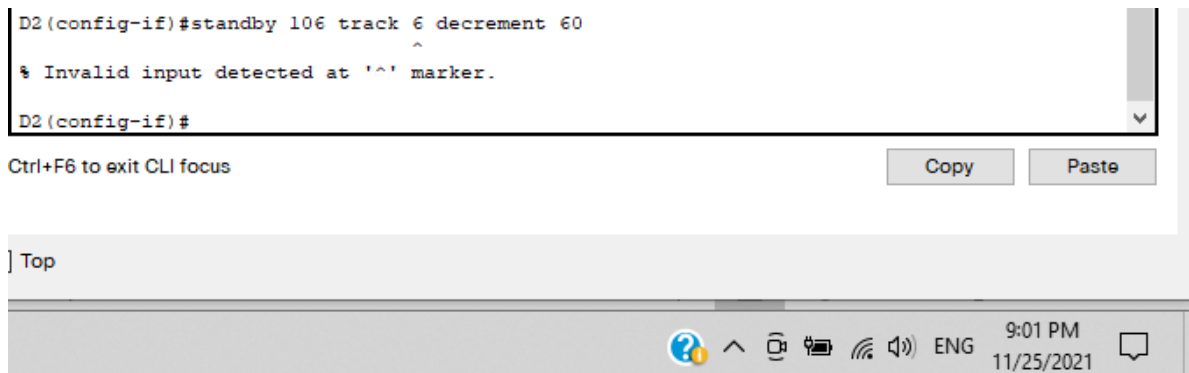
**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

- Asigne la dirección IP virtual usando IPv6 autoconfig.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

## Switch D2

```
D2 (config)# interface vlan 100
D2 (config-if)# standby 106 ipv6 autoconfig
D2 (config-if)#standby 106 preempt
%HSRP-6-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan 100 Grp 106 state Standby -> Active.
```



```
D2 (config-if)#standby 106 track 6 decrement 60
^
% Invalid input detected at '^' marker.
D2 (config-if)#
```

Figure 16 Ejecución IP SLA numero de rastreo 6 standby 106 en D2

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

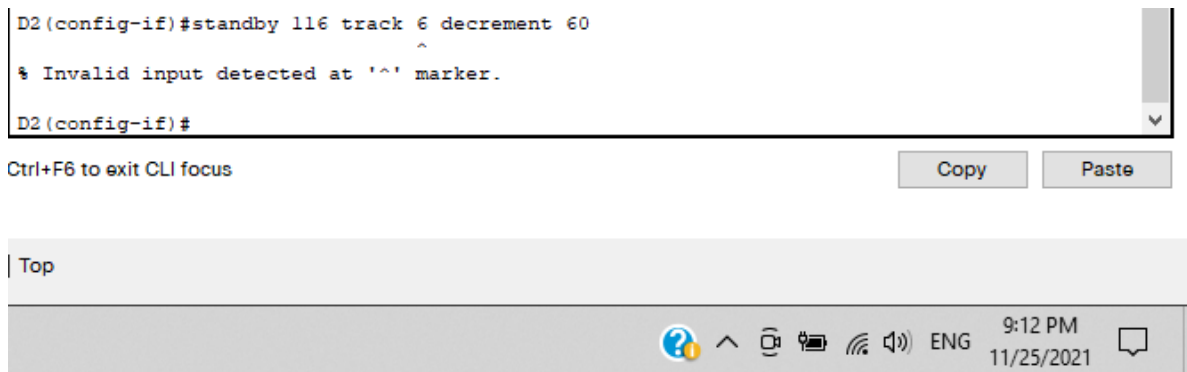
- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption)
- Rastree el objeto 6 para disminuir en 60.

## Switch D2

```
D2 (config)# interface vlan 101
```

```
D2 (config-if)# standby 116 ipv6 autoconfig
D2 (config-if)#standby 116 priority 150
%HSRP-6-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan 101 Grp 116 state Standby -> Active.

D2 (config-if)# standby 116 preempt
```



```
D2(config-if)#standby 116 track 6 decrement 60
^
% Invalid input detected at '^' marker.
D2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ENG 9:12 PM 11/25/2021

Figure 17 Ejecución IP SLA numero de rastreo 6 standby 116 en D2

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

### Switch D2

```
D2 (config)# interface vlan 102
D2 (config-if)# standby 126 ipv6 autoconfig
D2 (config-if)# standby 116 preempt

%HSRP-6-STATECHANGE: Vlan102 Grp 116 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan 102 Grp 116 state Standby -> Active.
```

```
D2(config-if)#standby 126 track 6 decrement 60
^
% Invalid input detected at '^' marker.
D2(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:46 PM 11/25/2021

Figure 18 Ejecución IP SLA numero de rastreo 6 standby 126 en D2

**Explicación:** Debido a que no se logró crear las IP SLAs el número de rastreo no está configurado y en esta instrucción no se puede continuar.

## Escenario 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

**5.1** En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

**Contraseña:** cisco12345cisco

```
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
^
% Invalid input detected at '^' marker.
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

10:16 PM 11/25/2021

Figure 19 Ejecucion Algorithm-type en R3

**Explicación:** En los routers R1, R2, R3 y A1 el comando *algorithm-type* no se encuentra disponible en la lista de comandos.

### Switch D1

```
D1 (config)# enable algorithm-type scrypt secret cisco12345cisco
```

### Switch D2

```
D2 (config)# enable algorithm-type scrypt secret cisco12345cisco
```

**5.2** En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

Detalles de la cuenta encriptada SCRYPT:

- Nombre de usuario local: **sadmin**.
- Nivel de privilegio **15**
- Contraseña: **cisco12345cisco**.

### Switch D1

```
D1 (config)# username sadmin privilege 15 algorithm-type scrypt secret  
cisco12345cisco
```

### Switch D2

```
D2 (config)# username sadmin privilege 15 algorithm-type scrypt secret  
cisco12345cisco
```

**Nota:** Este comando no se puede ejecutar en R1, R2, R3 y A1.

**5.3** En todos los dispositivos (excepto R2), habilite AAA.

- Habilite AAA.

### Router R1

```
R1(config)#aaa new-model
```

### Router R3

```
R3(config)#aaa new-model
```

### Switch D1

```
D1(config)#aaa new-model
```

### Switch D2

```
D2(config)#aaa new-model
```

## Switch A1

```
-----  
A1(config)#aaa new-model  
      ^  
% Invalid input detected at '^' marker.  
A1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ENG 11:39 PM 11/25/2021

Figure 20 Ejecución comando AAA en A1

**Explicación:** El switch A1 no permite ejecutar el comando aaa new-model.

**5.4** En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

Especificaciones del servidor RADIUS:

- Dirección IP del servidor RADIUS es 10.0.100.6
- Puertos UDP del servidor RADIUS son 1812 y 1813.
- Contraseña: \$trongPass

## Router R1

```
R1(config)# radius server RADIUS  
R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812  
R1(config-radius-server)# key $trongPass
```

```
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813  
      ^  
% Invalid input detected at '^' marker.  
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812  
R1(config-radius-server)#key $trongPass  
R1(config-radius-server)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ENG 11:57 PM 11/25/2021

Figure 21 Ejecución comando acct en R1

**Explicación:** El commando acct-port no se puede ejecutar.

### Router R3

```
R3(config)# radius server RADIUS
R3(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812
R3(config-radius-server)# key $trongPass
```

```
R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1646
% Invalid input detected at '^' marker.
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
R3(config-radius-server)#key $trongPass
R3(config-radius-server)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

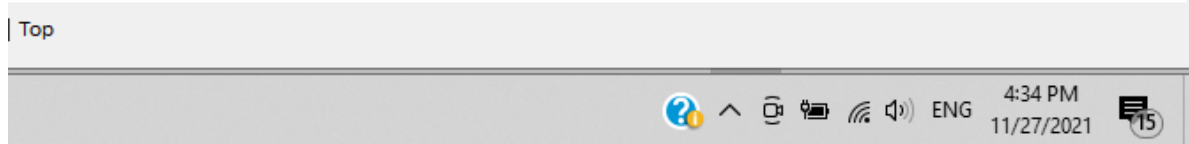


Figure 22 Ejecución comando acct en R3

**Explicación:** El commando acct-port no se puede ejecutar.

### Switch D1

```
D1(config)#radius server RADIUS
% Invalid input detected at '^' marker.
D1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste



Figure 23 Ejecución comando Radius Server en D1

**Explicación:** El comando radius no está disponible para un switch de capa 3.

## Switch D2

```
D2(config)#radius server RADIUS
      ^
% Invalid input detected at '^' marker.

D2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ENG 4:45 PM 11/27/2021

Figure 24 Ejecución comando Radius Server en D2

**Explicación:** El comando radius no está disponible para un switch de capa 3.

## Switch A1

```
A1(config)#radius server RADIUS
      ^
% Invalid input detected at '^' marker.

A1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

ENG 4:47 PM 11/27/2021

Figure 25 Ejecución comando Radius Server en A1

El comando radius no está disponible para un switch de capa 3.

**5.5** En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.

Especificaciones de autenticación AAA:

- Use la lista de métodos por defecto.
- Valide contra el grupo de servidores RADIUS.
- De lo contrario, utilice la base de datos local.

## Router R1

```
R1(config)# aaa authentication login default group radius local
```

### **Router R3**

```
R1(config)# aaa authentication login default group radius local
```

### **Switch D1**

```
D1(config)# aaa authentication login default group radius local
```

### **Switch D2**

```
D2(config)# aaa authentication login default group radius local
```

### **Switch A1**

```
A1(config)# aaa authentication login default group radius local
```

**5.6** Verifique el servicio AAA en todos los dispositivos (excepto R2)

Cierre e inicie sesión en todos los dispositivos (excepto R2) con el usuario: **raduser** y la contraseña: **upass123**.

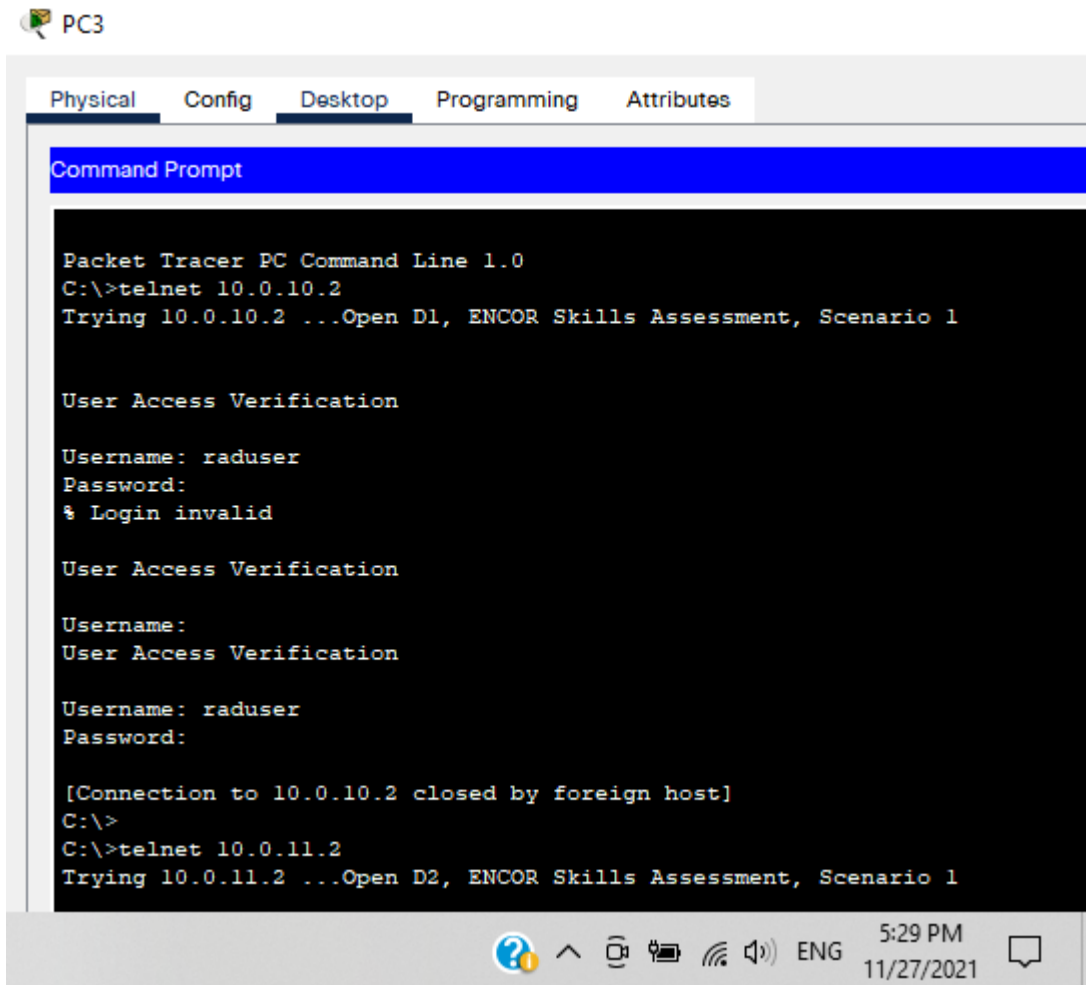


Figure 26 Verificación servicio AAA

**Explicación:** No todos los servicios se encuentran configurados por lo cual, al intentar verificar los servicios no es posible ingresar con el nombre y el usuario.

### **Escenario 6: Configure las funciones de Administración de Red**

En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

**6.1** En todos los dispositivos, configure el reloj local a la hora UTC actual

#### **Router R1**

**R1#** clock set 07:04:00 27 nov 2021

### **Router R2**

```
R2# clock set 07:08:00 27 nov 2021
```

### **Router R3**

```
R3# clock set 07:08:00 27 nov 2021
```

### **Switch D1**

```
D1# clock set 07:11:00 27 nov 2021
```

### **Switch D2**

```
D2# clock set 07:11:00 27 nov 2021
```

### **Switch A1**

```
A1# clock set 07:13:00 27 nov 2021
```

## **6.2 Configure R2 como un NTP maestro**

Configurar R2 como NTP maestro en el nivel de estrato 3.

### **Router R2**

```
R2(config)# ntp master 3
```

## **6.3 Configure NTP en R1, R3, D1, D2 y A1.**

Configure NTP de la siguiente manera:

- R1 debe sincronizar con R2.

### **Router R1**

```
R1(config)# ntp server 2.2.2.2
```

- R3, D1 y A1 para sincronizar la hora con R1.

### **Router R3**

```
R3(config)# ntp server 10.0.10.1
```

### **Switch D1**

```
D1(config)# ntp server 10.0.10.1
```

### **Switch A1**

```
A1(config)# ntp server 10.0.10.1
```

- D2 para sincronizar la hora con R3.

## Switch D2

```
D2 (config)# ntp server 10.0.11.1
```

### 6.4 Configure Syslog en todos los dispositivos excepto R2.

Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

## Router R1

```
R1(config)# logging host 10.0.100.5
```

```
R1(config)# logging on
```

```
R1(config)#logging trap warning
^
% Invalid input detected at '^' marker.
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

8:44 AM 11/28/2021

Figure 27 Ejecución nivel Warning en R1.

**Explicación:** *logging trap warning* no se encuentra disponible en la lista de comandos.

## Router R3

```
R1(config)# logging host 10.0.100.5
```

```
R1(config)# logging on
```

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#logging trap warning
^
% Invalid input detected at '^' marker.
```

8:49 AM 11/28/2021

Figure 28 Ejecución nivel Warning en R3

**Explicación:** *logging trap warning* no se encuentra disponible en la lista de comandos.

## Switch D1

```
D1(config)# logging host 10.0.100.5
D1(config)# logging on
```

```
D1(config)#logging trap warning
^
% Invalid input detected at '^' marker.
```

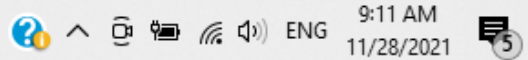


Figure 29 Ejecución nivel Warning en D1

**Explicación:** *logging trap warning* no se encuentra disponible en la lista de comandos.

## Switch D2

```
D2(config)# logging host 10.0.100.5
D2(config)# logging on
```

```
D2(config)#logging trap warning
^
% Invalid input detected at '^' marker.
```

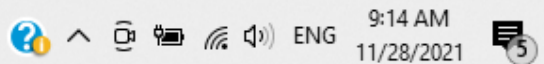


Figure 30 Ejecución nivel Warning en D2

**Explicación:** *logging trap warning* no se encuentra disponible en la lista de comandos.

## Switch A1

```
A1(config)# logging host 10.0.100.5
A1(config)# logging on
```

```
A1(config)#logging trap warning
^
% Invalid input detected at '^' marker.

A1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:16 AM 11/28/2021

Figure 31 Ejecución nivel Warning en A1

**Explicación:** *logging trap warning* no se encuentra disponible en la lista de comandos.

## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2.

Especificaciones de SNMPv2:

- Únicamente se usará SNMP en modo lectura.
- Limite el acceso SNMP a la dirección IP de la PC1.

### Router R1

```
R1(config)# ip access-list standard SNMP-NMS
R1(config-std-nacl) # permit host 10.0.100.5
R1(config-std-nacl) # exit
```

### Router R3

```
R3(config)# ip access-list standard SNMP-NMS
R3(config-std-nacl) # permit host 10.0.100.5
R3(config-std-nacl) # exit
```

### Switch D1

```
D1(config)# ip access-list standard SNMP-NMS
D1(config-std-nacl) # permit host 10.0.100.5
D1(config-std-nacl) # exit
```

### Switch D2

```
D2(config)# ip access-list standard SNMP-NMS
D2(config-std-nacl) # permit host 10.0.100.5
```

D2(config-std-nacl) # exit

### Switch A1

A1(config)# ip access-list standard SNMP-NMS

A1(config-std-nacl) # permit host 10.0.100.5

A1(config-std-nacl) # exit

- Configure el valor de contacto SNMP con su nombre

### Router R1

```
R1(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

9:35 AM 11/28/2021

Figure 32 Ejecución comando contact en R1

**Explicación:** El comando *contact* no se encuentra disponible en la lista.

### Router R3

```
R3(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.
R3(config)#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

9:37 AM 11/28/2021

Figure 33 Ejecución comando contact en R3

**Explicación:** El comando *contact* no se encuentra disponible en la lista.

## Switch D1

```
D1(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.
D1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:39 AM 11/28/2021

Figure 34 Ejecución comando contact en D1

**Explicación:** El comando *contact* no se encuentra disponible en la lista.

## Switch D2

```
D2(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.
D2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:40 AM 11/28/2021

Figure 35 Ejecución comando contact en D2

**Explicación:** El comando *contact* no se encuentra disponible en la lista.

## Switch A1

```
A1(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.
A1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:41 AM 11/28/2021

Figure 36 Ejecución comando contact en A1.

**Explicación:** El comando *contact* no se encuentra disponible en la lista.

- Establezca el *community string* en **ENCORSA**.

## Router R1

```
R1(config)#snmp-server community ENCORSA ro SNMP-NMS
^
% Invalid input detected at '^' marker.
R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:44 AM 11/28/2021

Figure 37 Ejecución comando SNMP-NMS en R1.

**Explicación:** El comando *SNMP-NMS* no se encuentra disponible en la lista.

## Router R3

```
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
^
% Invalid input detected at '^' marker.
R3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:46 AM 11/28/2021

Figure 38 Ejecución comando SNMP-NMS en R3.

**Explicación:** El comando *SNMP-NMS* no se encuentra disponible en la lista.

## Switch D1

```
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
^
% Invalid input detected at '^' marker.
D1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:47 AM 11/28/2021

Figure 39 Ejecución comando SNMP-NMS en D1.

**Explicación:** El comando *SNMP-NMS* no se encuentra disponible en la lista.

## Switch D2

```
D2(config)#snmp-server contact Cisco Student
^
% Invalid input detected at '^' marker.

D2(config)#snmp-server community ENCORSA ro SNMP-NMS
^
% Invalid input detected at '^' marker.

D2(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:48 AM 11/28/2021 ENG

Figure 40 Ejecución comando SNMP-NMS en D2.

**Explicación:** El comando *SNMP-NMS* no se encuentra disponible en la lista.

## Switch A1

```
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
^
% Invalid input detected at '^' marker.

A1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

9:50 AM 11/28/2021 ENG

Figure 41 Ejecución comando SNMP-NMS en A1.

**Explicación:** El comando *SNMP-NMS* no se encuentra disponible en la lista.

- En R3, D1 y D2 habilite el envío de *traps, config y ospf*.

### Router R3, D1 y D2

```
R3(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.

R3(config)#snmp-server enable traps ospf
^
% Invalid input detected at '^' marker.

R3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

9:56 AM 11/28/2021

Figure 42 Ejecución comando enable traps,config y ospf en R3,D1 y D2.

**Explicación:** El comando *SNMP-NMS enable* no se encuentra disponible en la lista.

- En R1, habilite el envío de *traps bgp,config y ospf*.

```
R1(config)#snmp-server enable traps bgp
^
% Invalid input detected at '^' marker.

R1(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.

R1(config)#snmp-server enable traps ospf
^
% Invalid input detected at '^' marker.

R1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

] Top

10:02 AM 11/28/2021

Figure 43 Ejecución comando enable traps,config y ospf en R3,D1 y D2.

**Explicación:** Los comandos *SNMP-NMS enable* no se encuentra disponible en la lista.

- En A1, habilite el envío de *traps config*.

### Switch A1

```
Al(config)#snmp-server enable traps config
^
% Invalid input detected at '^' marker.

Al(config)#snmp-server enable traps ospf
^
% Invalid input detected at '^' marker.

Al(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

10:09 AM 11/28/2021

Figure 44 Ejecución comando *enable traps,config* y *ospf* en A1.

**Explicación:** Los comandos *SNMP-NMS enable* no se encuentra disponible en la lista.

## CONCLUSIONES

El uso de Cisco Packet Tracer y GNS3 contrajo diferentes barreras tanto en la ejecución de comandos como en la ejecución del programa GNS3 en el computador, ya que es un software que consume un alto índice de la memoria RAM, lo que implica la adquisición de un computador de alto rendimiento, también al momento de ejecutar algunos comandos como la configuración DHCP en GNS3 se manejan de otro modo, por lo cual se escogió trabajar la topología en Cisco Packet Tracer.

La importancia de la configuración de la capa 2 radica en que esta proporciona la transferencia directa de datos entre dos dispositivos, para ello se requieren de múltiples configuraciones las cuales están relacionadas una después de la otra como es el caso de la configuración de los troncales IEEE 802.1 Q los cuales permiten el tráfico de las distintas VLAN o la creación de EtherChannels LACP los cuales dotan de velocidad a los switches, la velocidad total se balancea entre las interfaces, y cuando alguna se cae se balancea la carga entre las demás disponibles.

Para la configuración de los protocolos de enrutamiento como OSPF se comprende que este trabaja para redes más complejas tipo compañías de manera interna donde se requiere manejar el tráfico de la información de un punto a otro con direcciones IP y que por ello este tipo de protocolos pueden ser divididos en diferentes áreas para que el manejo de sus bases de datos por los diferentes routers sea más eficiente.

No se puede subestimar la importancia de la correcta configuración de los relojes en los dispositivos de red, es por eso que la configuración de NTP puede prevenir estos choques entre ellos, de esta forma se puede decir que a partir de los más sencillos se puede evitar inconvenientes a gran escala.

## BIBLIOGRAFIA

Alberto Rico. (2021). CCNA, la certificación de Cisco (cómo conseguirla). Noviembre 2021, de ambit Sitio web: <https://www.ambit-bst.com/blog/ccna-la-certificaci%C3%B3n-de-cisco-c%C3%B3mo-conseguirla>

Cisco Admin. (Feb 13 2020). Introduction to AAA Implementation. November 2021, de Cisco Sitio web: <https://learningnetwork.cisco.com/s/article/introduction-to-aaa-implementation#:~:text=By%20default%2C%20a%20Cisco%20IOS,a%20level%2015%20enable%20password.&text=The%20solution%20to%20this%20is,ability%20to%20an%20IOS%20device>.

CCNA desde Cero. (2019). STP: Diferencias y Similitudes con RSTP. Octubre 17/2021, de CCNA desde Cero Sitio web: <https://ccnadesdecero.com/curso/stp-vs-rstp/>

CCNA desde cero. (2021). RSTP: Conceptos. Noviembre 2021, de CCNA desde cero Sitio web: <https://ccnadesdecero.com/curso/rstp/>

FormaTalent Business School. (2021). Con qué elementos se desarrolla el CCNP en la ingeniería de redes. Noviembre 2021, de formatalent Sitio web: <https://formatalent.com/con-que-elementos-se-desarrolla-el-ccnp-en-la-ingenieria-de-redes/>

Lorena Fernández. (2020). Así puedes configurar un enlace trunk en un switch gestionable. 9 Agosto 2020, de RZ Redes Zone Sitio web: <https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/>

Sheldon. (2021). ¿Cuál es la diferencia entre el LACP y el PAGP?. Noviembre 2021, de Fs community Sitio web: <https://community.fs.com/es/blog/lacp-vs-pagp-comparison.html>