

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBAS DE HABILIDADES PRACTICAS CCNP

LEYDI MARCELA LOSADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

BOGOTA

2021

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBAS DE HABILIDADES PRACTICAS CCNP

LEYDI MARCELA LOSADA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO  
DE INGENIERÍA DE TELECOMUNICACIONES

Director

MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

BOGOTA

2021

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

BOGOTA, (noviembre 28, 2021)

## **AGRADECIMIENTO**

Agradecimiento en especial a mi familia que me ha brindado todo el apoyo incondicional en este proceso de formación profesional como ingeniero electrónico. De igual modo, agradezco a todos mis compañeros y tutores por el compromiso y acompañamiento oportuno.

Finalmente, mi agradecimiento a la Universidad Nacional Abierta a Distancia (UNAD) y a su extenso equipo de trabajo, sin este método de formación, muchas personas no podrían optar por una educación superior. Agradezco sinceramente todo el apoyo y espacio de formación, espero seguir perteneciendo a esta gran familia y ser parte de su futuro.

## CONTENIDO

AGRADECIMIENTO	4
LISTA DE FIGURAS	6
GLOSARIO	7
RESUMEN	8
ABSTRACT	9
INTRODUCCION	10
ESCENARIO 1	11
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	11
Parte 2: Configurar la capa 2 de la red y el soporte de Host	21
Parte 3: Configurar los protocolos de enrutamiento	33
Parte 4: Configurar la Redundancia de Primer Salto(Fist Hop Redundancy)	43
Parte 5: Seguridad	50
Parte 6: Configure las funciones de Administración de Red	53
CONCLUSIONES	57
BIBLIOGRAFIA	58

## LISTA DE FIGURAS

FIGURA 1 TOPOLOGÍA DE RED ESCENARIO 1 .....	11
FIGURA 2 HOST PC 1 .....	20
FIGURA 3 HOST PC 4 .....	21
FIGURA 4 DHCP PC2 .....	25
FIGURA 5 FASTETHERNET 0.....	26
FIGURA 6 DHCP PC3 .....	27
FIGURA 7 DHCP PC3 FSDTETHERNET10.....	28
FIGURA 8 VERIFICACIÓN LAN LOCAL .....	29
FIGURA 9 VERIFICACIÓN D2: 10.0.100.2 .....	30
FIGURA 10 PC2 PING D1: 10.0.102.1 D2: 10.0.102.2.....	31
FIGURA 11 PC3 PING D1: 10.0.102.1 D2: 10.0.102.2.....	32
FIGURA 12 PC4 PING D1: 10.0.102.1 D2: 10.0.102.2: PC1: 10.0.100.5 .....	33

## GLOSARIO

**Dirección IP:** Una dirección en la red asignada a una interfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

**EtherChannels:** permite la agrupación lógica de varios enlaces físicos ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico ethernet usado y así obtener un enlace troncal de alta velocidad.

**ROUTER:** permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

**Shutdown:** Permite apagar o reiniciar un equipo local o remoto. El comando shutdown, utilizado sin parámetros, cierra la sesión del usuario actual.

**VLAN:** Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

## RESUMEN

En el siguiente trabajo se desarrollaron escenarios relacionados con diferentes aspectos de la red de datos de la plataforma Cisco, y se describen en detalle las etapas ejecutadas en cada etapa; las capturas de pantalla apoyan este escenario, que se logra mediante La interfaz de red específica implementa el protocolo de asignación de VLAN demostrar que el uso de equipos electrónicos para realizar el intercambio de señales de red desde la fuente al destino deseado es la parte básica de la interconexión de computadoras y dispositivos periféricos.

Al aplicar comandos de configuración a diferentes tipos de dispositivos activos, recuperar conocimientos previos y realizar una implementación avanzada de protocolos de enrutamiento nos ayudará a mejorar nuestra experiencia como profesionales en el futuro.

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



## **ABSTRACT**

In the following work, scenarios related to different aspects of the Cisco platform data network were developed, and the steps executed at each stage are described in detail; the screenshots support this scenario, which is achieved by The specific network interface implements the VLAN assignment protocol demonstrate that the use of electronic equipment to perform the exchange of network signals from the source to the desired destination is the basic part of the interconnection of computers and peripheral devices.

By applying configuration commands to different types of active devices, retrieving previous knowledge and performing advanced implementation of routing protocols will help us improve our expertise as professionals in the future.

**Keywords:** CISCO, CCNP, Routing, Swicthing, Networking, Electronics

## INTRODUCCION

En el transcurso del tiempo la tecnología se ha convertido en una parte fundamental de nuestras vidas, ayudándonos a comprender y responder a cada una de las incógnitas que se nos presentan, puesto que sin duda el internet ha transformado el mundo, su continuo avance está revolucionando el mundo y la manera de verlo.

En el siguiente trabajo se desarrolla la fase final del curso diplomado de profundización en CCNP llamado “prueba de habilidades prácticas”, para dicha fase se obtuvo el apoyo del programa Cisco Packet tracer el cual es parte fundamental a la hora de la programación de cada tarea y escenario que se presentan en la guía de trabajo. Además; se encontrarán ejercicios del módulo CCNP ROUTE donde se pondrán a prueba los conocimientos acerca de los protocolos de enrutamiento EIGRP, OSPF, EBGp y la redistribución de rutas que existe entre ellos, así mismo, se presenta un ejercicio relacionado con el módulo CCNP SWITCH donde se aplicarán los conceptos adquiridos a lo largo del curso. Durante su desarrollo se soluciona un escenario dividido en dos que se emplean los protocolos de enrutamiento que se les realiza una configuración avanzada para que exista una comunicación de extremo a extremo, Al final se espera adquirir las habilidades y competencias necesarias para la implementación de una red tipo campus según las competencias proyectadas para el final del curso.

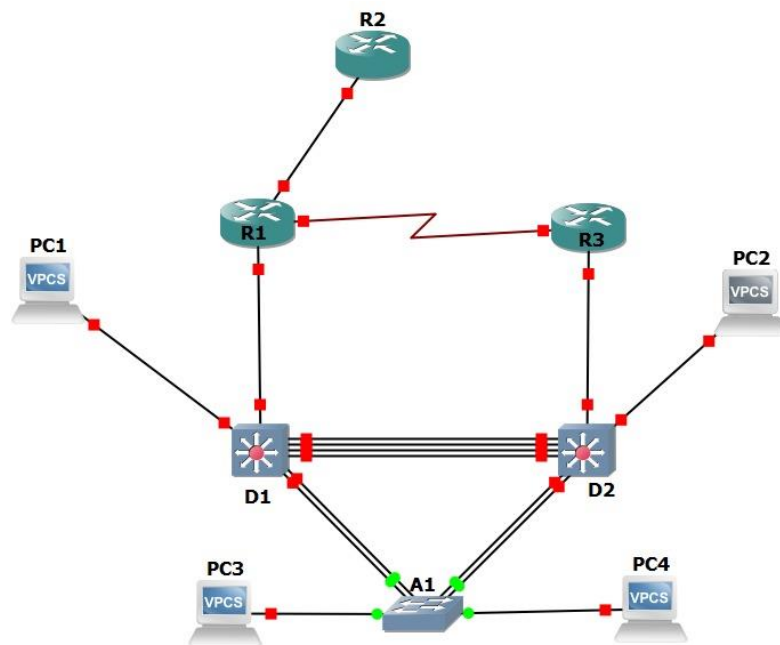
Finalmente, por medio de la plataforma de Cisco Networking Academy, se obtiene un contenido significativo para el desarrollo del diplomado de profundización CCNP el cual es muy importante, ya que proporciona un gran aporte para nuestro crecimiento laboral, el cual mejorará nuestro desempeño a nivel profesional, al involucrarnos en el mundo del Networking.

## ESCENARIO 1

**Parte 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 red escenario 1



*Fuente: tomado de Prueba de habilidades Ccnp 2021, Cisco Academy*

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

### Router R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
```

```
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
interface F0/0
  ip address 209.165.200.225 255.255.255.224
  ipv6 address fe80::1:1 link-local
  ipv6 address 2001:db8:200::1/64
  no shutdown
  exit
interface F0/1
  ip address 10.0.10.1 255.255.255.0
  ipv6 address fe80::1:2 link-local
  ipv6 address 2001:db8:100:1010::1/64
  no shutdown
  exit
interface s2/0
  ip address 10.0.13.1 255.255.255.0
  ipv6 address fe80::1:3 link-local
  ipv6 address 2001:db8:100:1013::1/64
  no shutdown
  exit
```

## **Router R2**

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
```

```
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

### **Router R3**

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
```

```
exit
interface s0/1/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

### **Switch D1**

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
```

```
interface g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
```

```
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10
shutdown
exit
interface range g1/0/12-24
shutdown
exit
interface range g1/1/1-4
shutdown
exit
```

## **Switch D2**

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
```



```
vlan 101
  name UserGroupA
  exit
vlan 102
  name UserGroupB
  exit
vlan 999
  name NATIVE
  exit
interface g1/0/11
  no switchport
  ip address 10.0.11.2 255.255.255.0
  ipv6 address fe80::d1:1 link-local
  ipv6 address 2001:db8:100:1011::2/64
  no shutdown
  exit
interface vlan 100
  ip address 10.0.100.2 255.255.255.0
  ipv6 address fe80::d2:2 link-local
  ipv6 address 2001:db8:100:100::2/64
  no shutdown
  exit
interface vlan 101
  ip address 10.0.101.2 255.255.255.0
  ipv6 address fe80::d2:3 link-local
  ipv6 address 2001:db8:100:101::2/64
  no shutdown
  exit
interface vlan 102
  ip address 10.0.102.2 255.255.255.0
```

```
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10
shutdown
exit
interface range g1/0/12-24
shutdown
exit
interface range g1/1/1-4
shutdown
exit
```

### **Switch A1**

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
```

```
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
exit
```

**Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.**

Figura 2 host PC 1

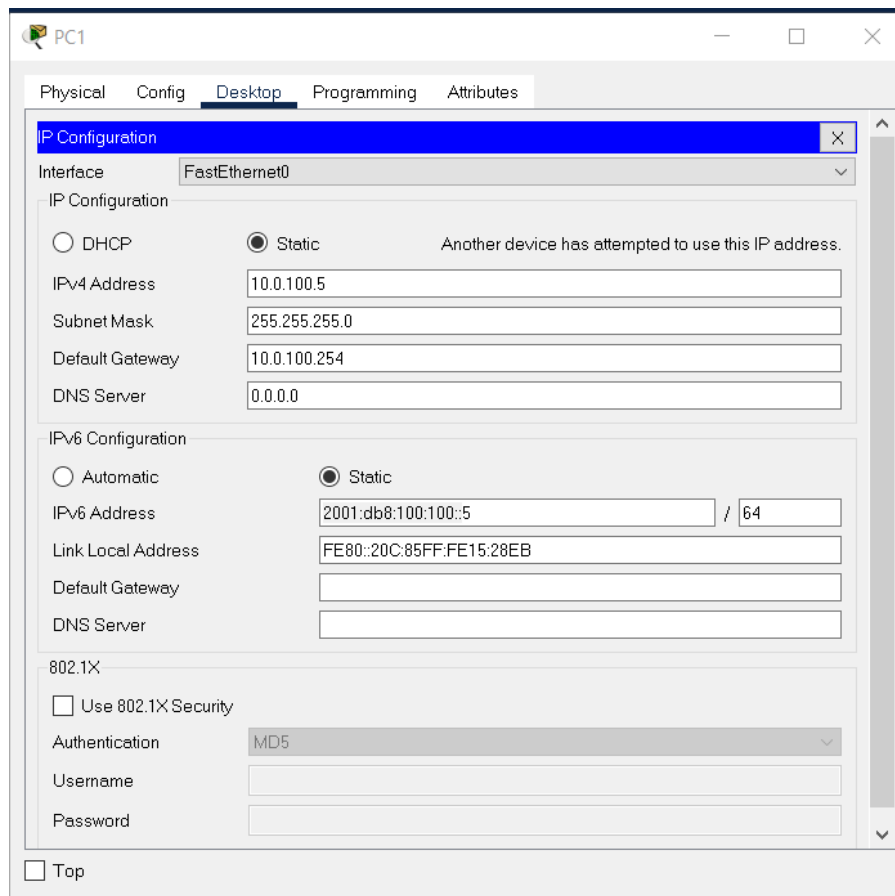
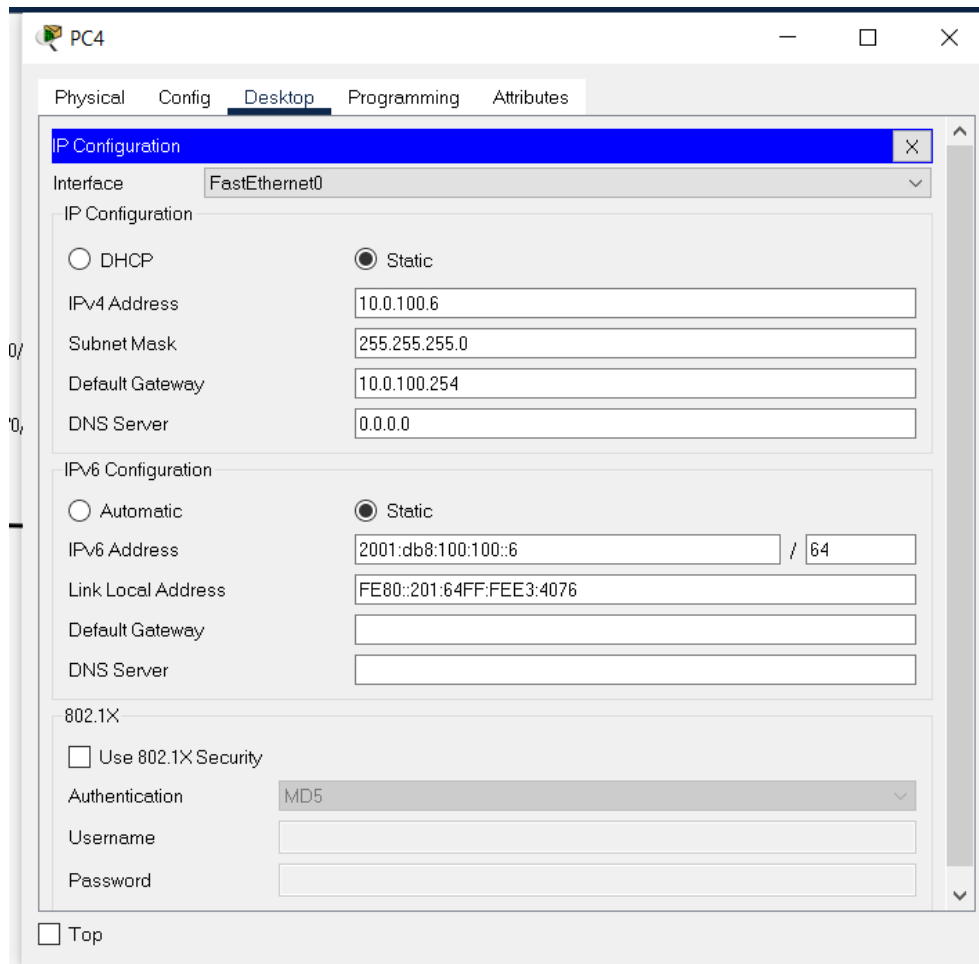


Figura 3 host PC 4



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

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

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

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

```
D2(config)#interface range gigabitEthernet 1/0/1 - 6
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
```

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

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

```
D1(config-if-range)#switchport trunk native vlan 999
```

```
D2(config-if-range)#switchport trunk native vlan 999
```

```
A1(config-if-range)#switchport trunk native vlan 999
```

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

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

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

```
A1(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).**

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

```
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100 root secondary
D2(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 g1/0/1-4
D1(config-if-range)# channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D1(config-if-range)# no shutdown
```

```
D2(config)# interface range g1/0/1-4
D2(config-if-range)# channel-group 12 mode passive
Creating a port-channel interface Port-channel 12
D2(config-if-range)# no shutdown
```

**• D1 a A1 – Port channel 1**

```
D1(config)# interface range g1/0/5-6
D1(config-if-range)# channel-group 1 mode active
```

Creating a port-channel interface Port-channel 1  
D1(config-if-range)# no shutdown

A1(config)# interface range f0/1-2  
A1(config-if-range)# channel-group 1 mode passive  
Creating a port-channel interface Port-channel 1  
A1(config-if-range)# no shutdown

• **D2 a A1 – Port channel 2**

D2(config)# interface range g1/0/5-6  
D2(config-if-range)# channel-group 2 mode active  
Creating a port-channel interface Port-channel 2  
D2(config-if-range)# no shutdown

A1(config)# interface range f0/3-4  
A1(config-if-range)# channel-group 2 mode passive  
Creating a port-channel interface Port-channel 2  
A1(config-if-range)# no shutdown

**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.**

D1(config)# interface g1/0/23  
D1(config-if)# switchport mode Access  
D1(config-if)# switchport Access vlan 100  
D1(config-if)# no shutdown  
D2(config)# interface g1/0/23  
D2(config-if)# switchport mode Access  
D2(config-if)# switchport Access vlan 102



D2(config-if)# no shutdown

A1(config)# interface f0/23

A1(config-if)# switchport mode Access

A1(config-if)# switchport Access vlan 101

A1(config-if)# no shutdown

A1(config)# interface f0/24

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.

Figura 4 DHCP pc2

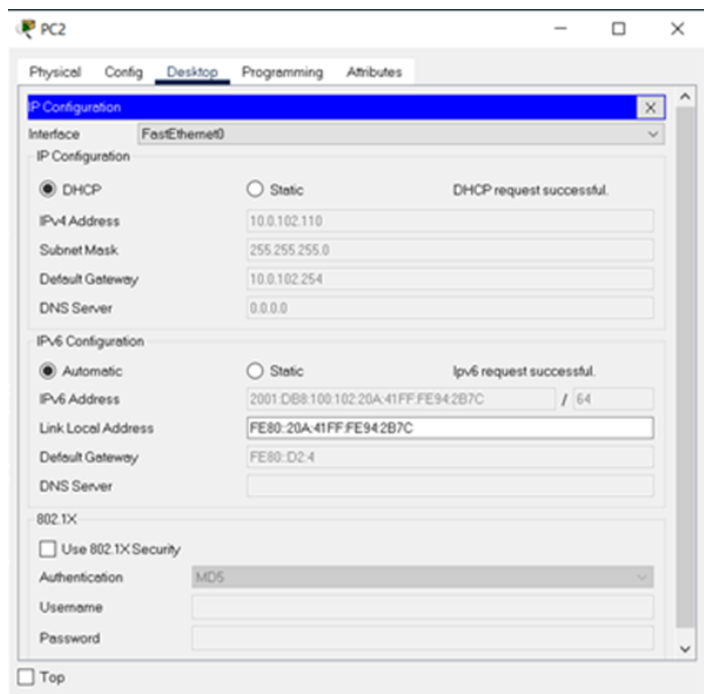


Figura 5 FastEthernet 0

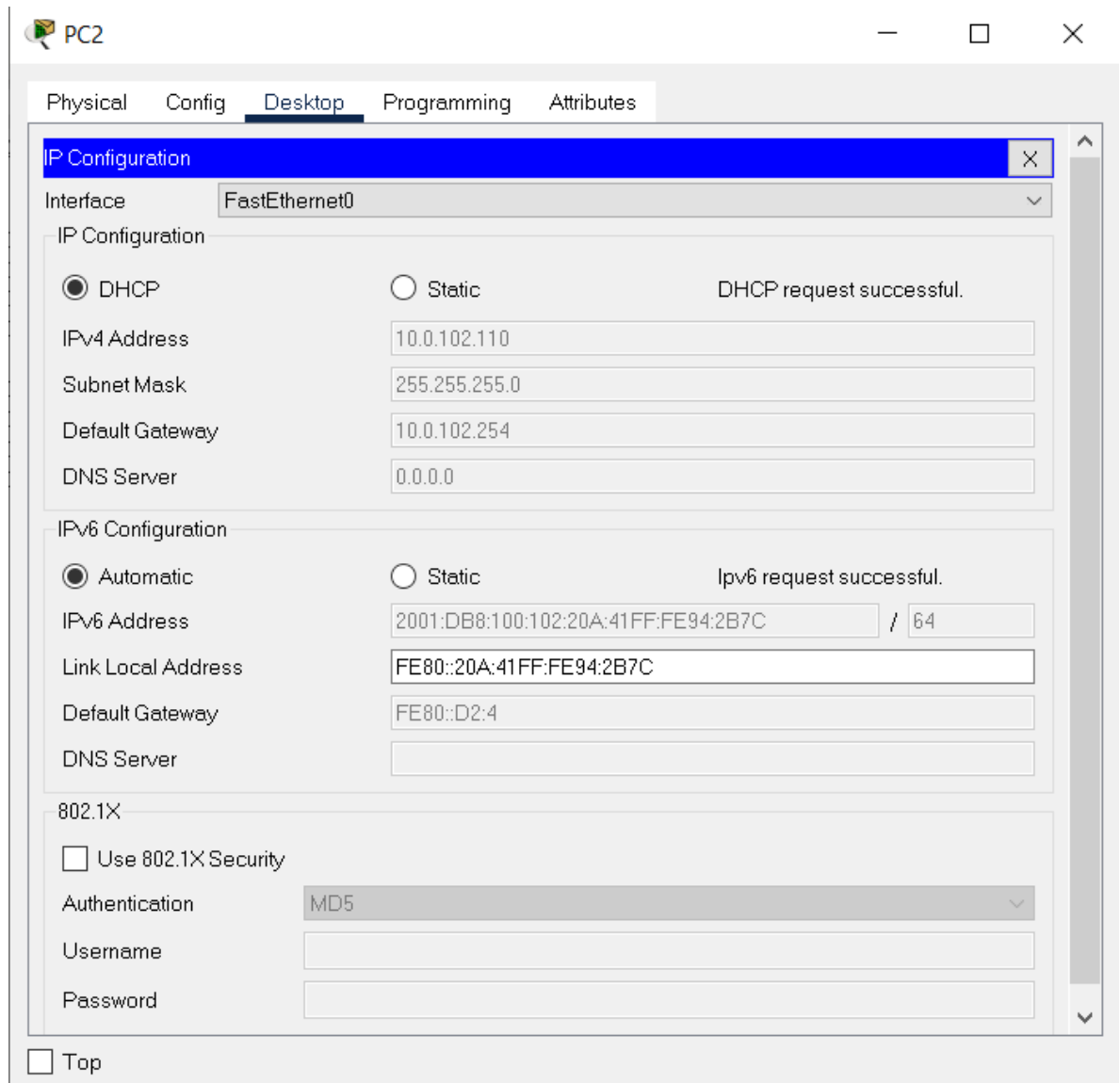


Figura 6 DHCP pc3

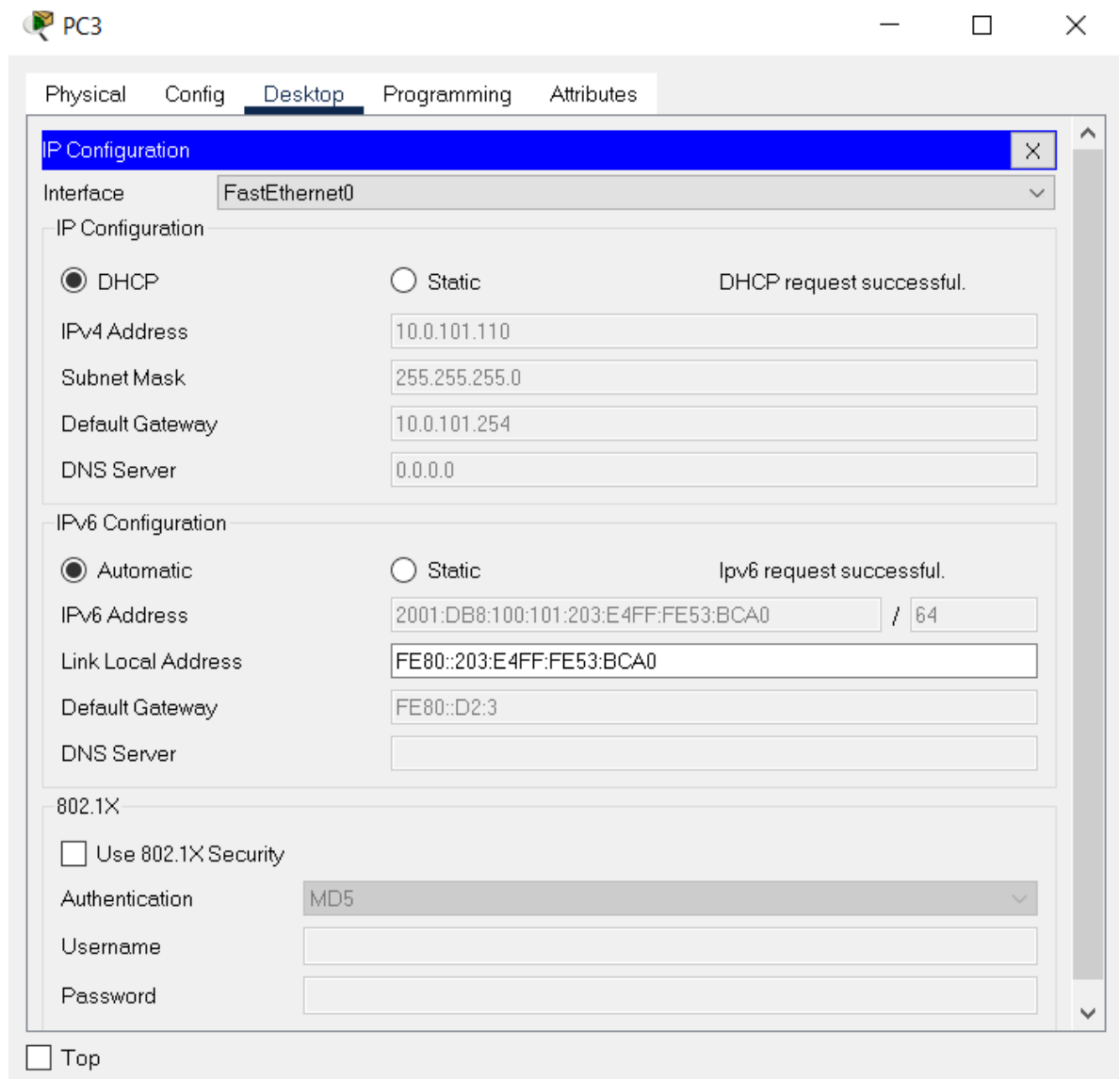
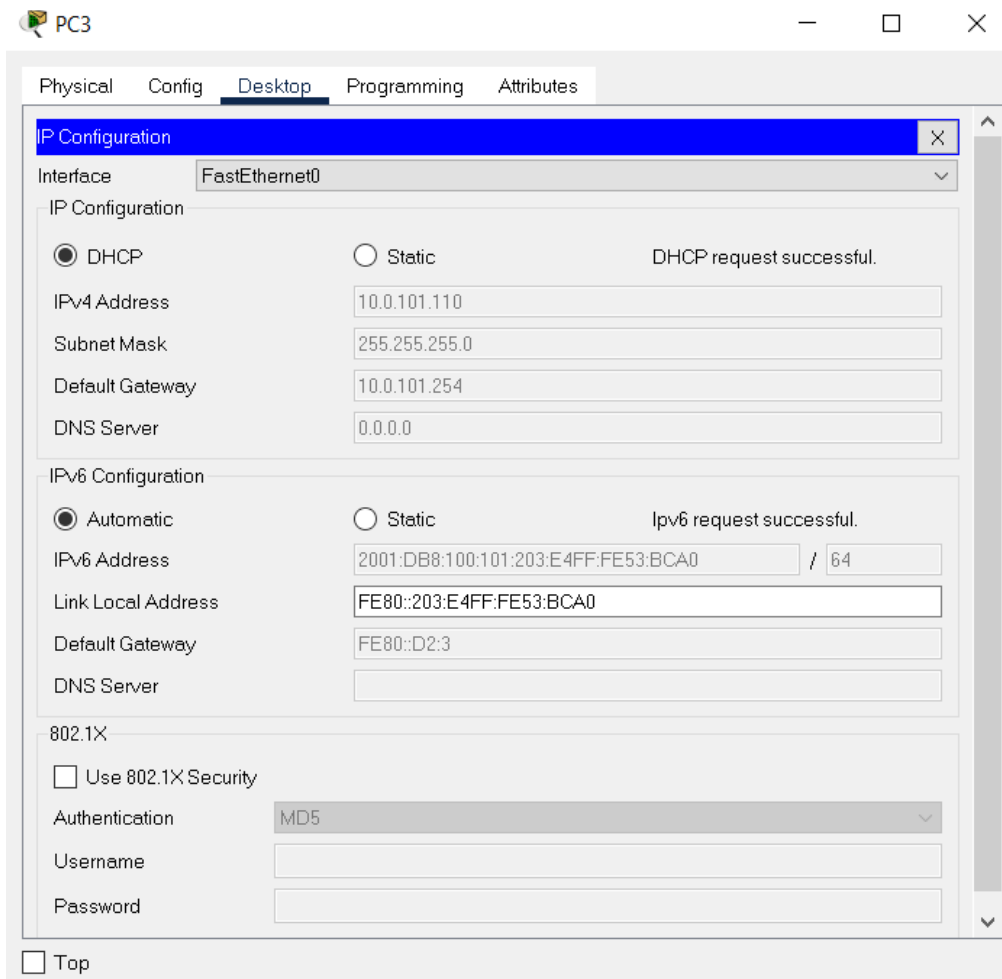


Figura 7 DHCP pc3 Fsdtdethernet10



Verifique la conectividad de la LAN local PC1 debería hacer ping con éxito a:

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

Figura 8 Verificación LAN local

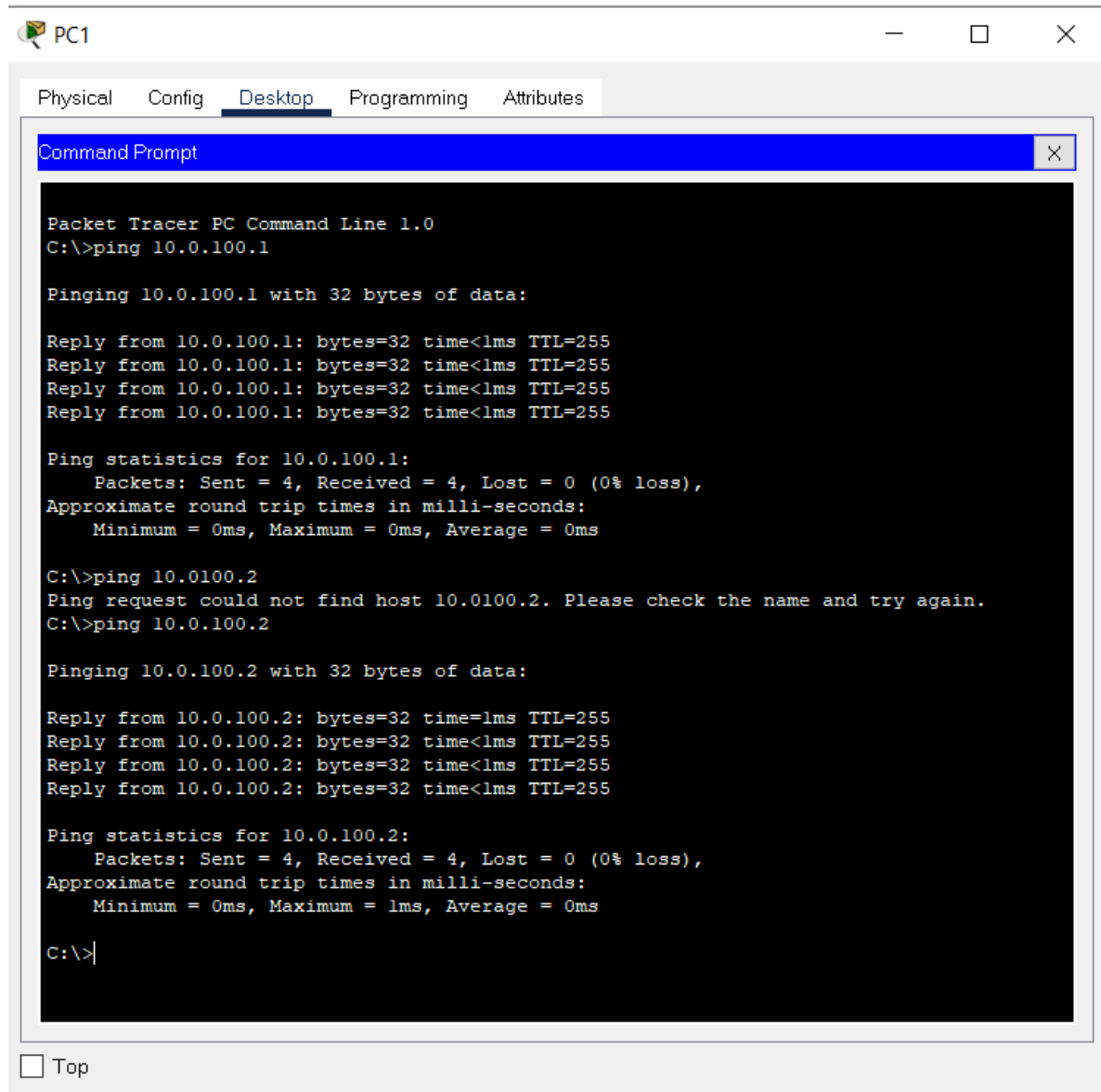
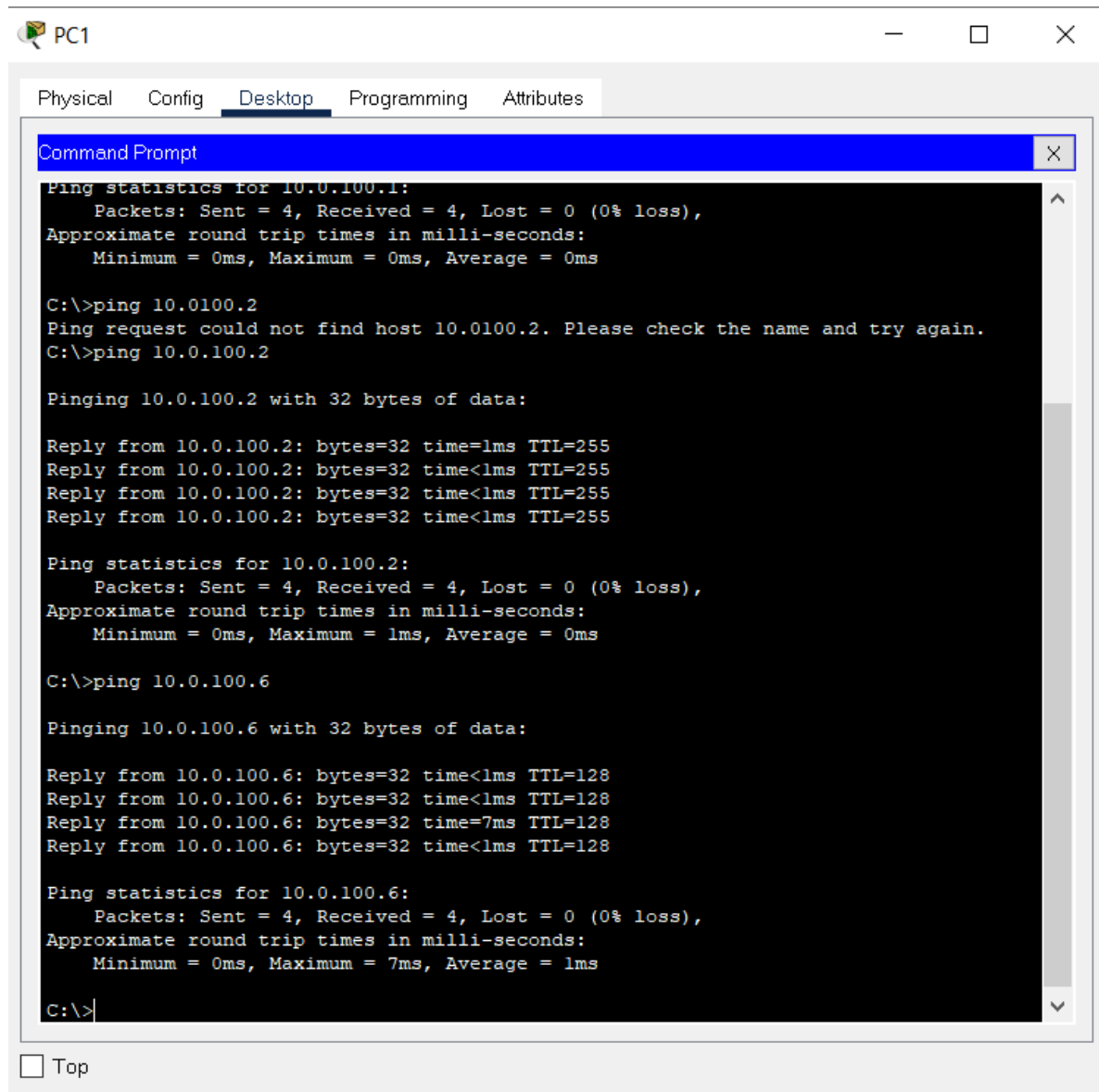


Figura 9 Verificación D2: 10.0.100.2



The screenshot shows a Windows PC1 desktop with a Command Prompt window open. The window title is "Command Prompt" and it has a blue header bar. The desktop background is black. The Command Prompt shows the following text:

```
Physical Config Desktop Programming Attributes
Command Prompt
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 = 0ms, Average = 0ms

C:\>ping 10.0100.2
Ping request could not find host 10.0100.2. Please check the name and try again.
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 10.0.100.6

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=7ms 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 = 7ms, Average = 1ms

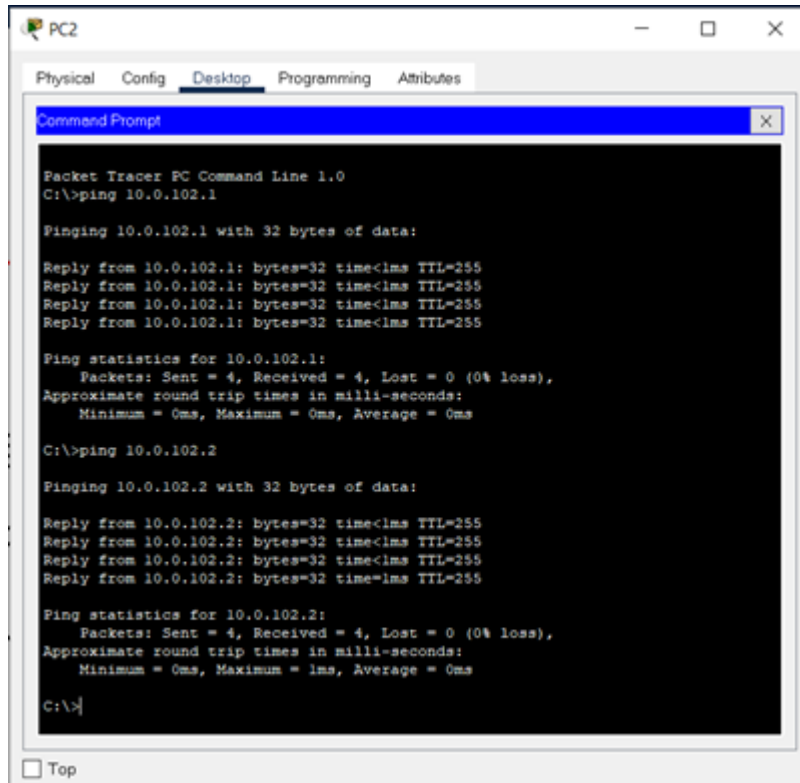
C:\>
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

PC2 debería hacer ping con éxito a:

- D1: 10.0.102.1
- D2: 10.0.102.2

Figura 10 PC2 ping D1: 10.0.102.1 D2: 10.0.102.2



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
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<ms TTL=255
Reply from 10.0.102.1: bytes=32 time<ms TTL=255
Reply from 10.0.102.1: bytes=32 time<ms TTL=255
Reply from 10.0.102.1: bytes=32 time<ms 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 = 0ms, Average = 0ms

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

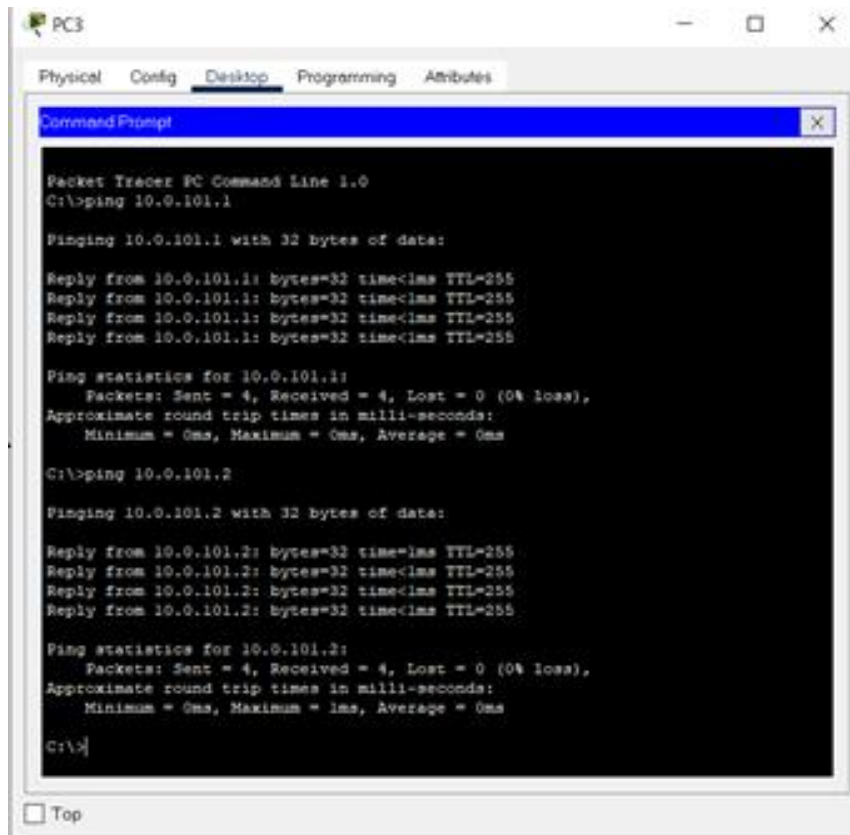
Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

PC3 debería hacer ping con éxito a:

- D1: 10.0.101.1
- D2: 10.0.101.2

Figura 11 PC3 ping D1: 10.0.102.1 D2: 10.0.102.2



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
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<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
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 = 0ms, Average = 0ms

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 = 1ms, Average = 0ms

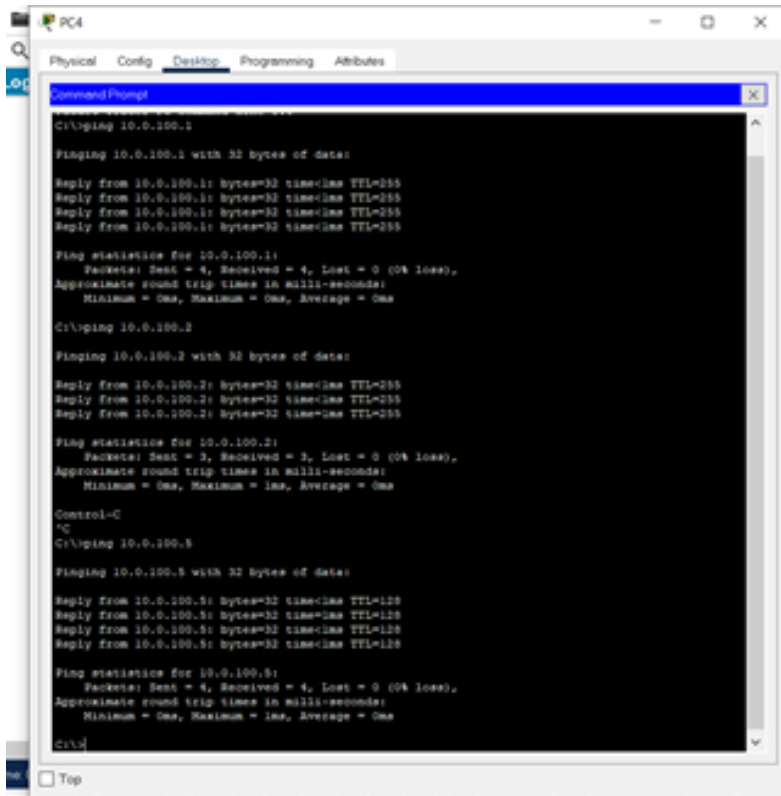
C:\>
```

PC4 debería hacer ping con éxito a:

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



Figura 12 PC4 ping D1: 10.0.102.1 D2: 10.0.102.2: PC1: 10.0.100.5



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
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=1ms 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 = 0ms, Average = 0ms

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

Ping statistics for 10.0.100.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
^C
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 = 1ms, Average = 0ms

C:\>
```

### Parte 3: Configurar los protocolos de enrutamiento

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2

En área 0.

Use OSPF Process ID 4 y asigne los siguientes routerIDs:

- R1: 0.0.4.1  
R1(config)#router ospf 4  
R1(config-router)#router-id 0.0.4.1

- R3: 0.0.4.3  
R3(config)#router ospf 4  
R3(config-router)#router-id 0.0.4.1
- D1: 0.0.4.131  
D1(config)#router ospf 4  
D1(config-router)#router-id 0.0.4.131
- D2: 0.0.4.132  
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 Area 0.**

- **En R1, no publique la red R1 – R2.**  
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  
  
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  
  
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0  
D1(config-router)#network 10.0.100.0 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  
  
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0  
D2(config-router)#network 10.0.100.0 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

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

```
R1(config-router)#default-information originate
```

Deshabilite las publicaciones OSPFv2 en:

- **D1: todas las interfaces excepto G1/0/11**

```
D1(config-router)#passive-interface gigabitEthernet 1/0/1
D1(config-router)#passive-interface gigabitEthernet 1/0/2
D1(config-router)#passive-interface gigabitEthernet 1/0/3
D1(config-router)#passive-interface gigabitEthernet 1/0/4
D1(config-router)#passive-interface gigabitEthernet 1/0/5
D1(config-router)#passive-interface gigabitEthernet 1/0/6
D1(config-router)#passive-interface gigabitEthernet 1/0/7
D1(config-router)#passive-interface gigabitEthernet 1/0/8
D1(config-router)#passive-interface gigabitEthernet 1/0/9
D1(config-router)#passive-interface gigabitEthernet 1/0/10
D1(config-router)#passive-interface gigabitEthernet 1/0/12
D1(config-router)#passive-interface gigabitEthernet 1/0/13
D1(config-router)#passive-interface gigabitEthernet 1/0/14
D1(config-router)#passive-interface gigabitEthernet 1/0/15
D1(config-router)#passive-interface gigabitEthernet 1/0/16
D1(config-router)#passive-interface gigabitEthernet 1/0/17
D1(config-router)#passive-interface gigabitEthernet 1/0/18
D1(config-router)#passive-interface gigabitEthernet 1/0/19
D1(config-router)#passive-interface gigabitEthernet 1/0/20
D1(config-router)#passive-interface gigabitEthernet 1/0/21
D1(config-router)#passive-interface gigabitEthernet 1/0/22
D1(config-router)#passive-interface gigabitEthernet 1/0/23
```

D1(config-router)#passive-interface gigabitEthernet 1/0/24

- **D2: todas las interfaces excepto G1/0/11**

D2(config-router)#passive-interface gigabitEthernet 1/0/1  
D2(config-router)#passive-interface gigabitEthernet 1/0/2  
D2(config-router)#passive-interface gigabitEthernet 1/0/3  
D2(config-router)#passive-interface gigabitEthernet 1/0/4  
D2(config-router)#passive-interface gigabitEthernet 1/0/5  
D2(config-router)#passive-interface gigabitEthernet 1/0/6  
D2(config-router)#passive-interface gigabitEthernet 1/0/7  
D2(config-router)#passive-interface gigabitEthernet 1/0/8  
D2(config-router)#passive-interface gigabitEthernet 1/0/9  
D2(config-router)#passive-interface gigabitEthernet 1/0/10  
D2(config-router)#passive-interface gigabitEthernet 1/0/12  
D2(config-router)#passive-interface gigabitEthernet 1/0/13  
D2(config-router)#passive-interface gigabitEthernet 1/0/14  
D2(config-router)#passive-interface gigabitEthernet 1/0/15  
D2(config-router)#passive-interface gigabitEthernet 1/0/16  
D2(config-router)#passive-interface gigabitEthernet 1/0/17  
D2(config-router)#passive-interface gigabitEthernet 1/0/18  
D2(config-router)#passive-interface gigabitEthernet 1/0/19  
D2(config-router)#passive-interface gigabitEthernet 1/0/20  
D2(config-router)#passive-interface gigabitEthernet 1/0/21  
D2(config-router)#passive-interface gigabitEthernet 1/0/22  
D2(config-router)#passive-interface gigabitEthernet 1/0/23  
D2(config-router)#passive-interface gigabitEthernet 1/0/24

**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 routerIDs:

- R1: 0.0.6.1  
R1(config)#ipv6 unicast-routing  
R1(config)#ipv6 router ospf 6  
R1(config-rtr)#router-id 0.0.6.1
  
- R3: 0.0.6.3  
R3(config)#ipv6 unicast-routing  
R3(config)#ipv6 router ospf 6  
R3(config-rtr)#router-id 0.0.6.3
  
- D1: 0.0.6.131  
D1(config)#ipv6 unicast-routing  
D1(config)#ipv6 router ospf 6  
D1(config-rtr)#router-id 0.0.6.131
  
- D2: 0.0.6.132  
D2(config)#ipv6 unicast-routing  
D2(config)#ipv6 router ospf 6  
D2(config-rtr)#router-id 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.

```
R1(config)#int g 0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#int s 0/1/0
R1(config-if)#ipv6 ospf 6 area 0
```

```
R3(config)#int g 0/0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#int s 0/1/0
R3(config-if)#ipv6 ospf 6 area 0
```

```
D1(config)#int g 1/0/11
D1(config-if)#ipv6 ospf 6 area 0
D1(config)#int vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config)#int vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config)#int vlan 102
D1(config-if)#ipv6 ospf 6 area 0
```

```
D2(config)#int g 1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config)#int vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config)#int vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config)#int vlan 102
D2(config-if)#ipv6 ospf 6 area 0
```

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

R1(config-rtr)#default-information originate

Deshabilite las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto G1/0/11  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/2  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/3  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/4  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/5  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/6  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/7  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/8  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/9  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/10  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/12  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/13  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/14  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/15  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/16  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/17  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/18  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/19  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/20  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/21  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/22  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/23  
D1(config-rtr)#passive-interface gigabitEthernet 1/0/24

- D2: todas las interfaces excepto G1/0/11
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/2
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/3
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/4
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/5
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/6
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/7
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/8
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/9
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/10
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/12
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/13
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/14
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/15
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/16
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/17
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/18
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/19
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/20
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/21
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/22
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/23
  - D2(config-rtr)#passive-interface gigabitEthernet 1/0/24

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

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

- Una ruta estática predeterminada IPv4.
  - R2(config)#ip route 0.0.0.0 0.0.0.0 0.0.0.0



- Una ruta estática predeterminada IPv6.

```
R2(config)#ipv6 route 0::0/64 0::0
```

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

```
R2(config)#router bgp 500
```

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

```
R2(config-router)# neighbor 209.165.200.225 remote-as 300
```

```
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300
```

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

En IPv4 address family, anuncie:

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0).

```
R2(config-router)# address-family ipv4
```

```
R2(config-router-af)# neighbor 209.165.200.225 activate
```

```
R2(config-router-af)# no neighbor 2001:db8:200::1 activate
```

```
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255
```

```
R2(config-router-af)# network 0.0.0.0
```

```
R2(config-router-af)# exit-address-family
```

En IPv6 address family, anuncie:

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

```
R2(config-router)#address-family ipv6
```

```
R2(config-router-af)# no neighbor 209.165.200.225 activate
```

```
R2(config-router-af)# neighbor 2001:db8:200::1 activate
```

```
R2(config-router-af)# network 2001:db8:2222::/128
```

```
R2(config-router-af)# network ::/0
```

```
R2(config-router-af)# exit-address-family
```

### 3.4 En R1 en la “Red ISP”, configure MPBGP

Configure dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.  
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
- Una ruta resumen IPv6 para 2001:db8:100::/48.  
R1(config)#ipv6 route 2001:db8:100::/48 null0

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

```
R1(config)#router bgp 300
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# neighbor 209.165.200.226 remote-as 500
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500
```

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

- Deshabilite la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.  
R1(config-router)# address-family ipv4 unicast  
R1(config-router-af)# neighbor 209.165.200.226 activate  
R1(config-router-af)# no neighbor 2001:db8:200::2 activate  
R1(config-router-af)# exit-address-family
- Anuncie la red 10.0.0.0/8.  
R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.

```
R1(config-router)# address-family ipv6 unicast
```

```
R1(config-router-af)# no neighbor 209.165.200.226 activate
```

```
R1(config-router-af)# neighbor 2001:db8:200::2 activate
```

```
R1(config-router-af)# exit-address-family
```

- Anuncie la red 2001:db8:100::/48.

```
R1(config-router-af)# network 2001:db8:100::/48
```

#### **Parte 4: Configurar la Redundancia de Primer Salto(Fist Hop Redundancy)**

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

- Use la SLA numero 4 para IPv4.
- Use la SLA numero 6 para IPv4.

```
D1# show run
```

```
D1(config)# track 4 ip sla 4
```

```
D1(config)# delay down 10 up 15
```

```
D1(config)# track 6 ip sla 6
```

```
D1(config)# delay down 10 up 15
```

```
D1(config)# ip sla
```

```
D1(config-ip-sla) icmp-echo 10.0.10.1
```

```
D1(config-ip-sla-echo)frequency 5
```

```
D1(config-ip-sla-echo)# exit
```

```
D1(config)# ip sla schedule 4 life forever start-time now
```

```
D1(config)# ip sla 6
```

```
D1(config-ip-sla) icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)frequency 5
D1(config-ip-sla-echo)# exit
D1(config)# ip sla schedule 6 life forever start-time now
```

#### 4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1

- Use la SLA numero 4 para IPv4.
- Use la SLA numero 6 para IPv4.

```
D2# show run
D2(config)# track 4 ip sla 4
D2(config)# delay down 10 up 15
D2(config)# track 6 ip sla 6
D2(config)# delay down 10 up 15
D2(config)# ip sla
D2(config-ip-sla) icmp-echo 10.0.10.1
D2(config-ip-sla-echo)frequency 5
D2(config-ip-sla-echo)# exit
D2(config)# ip sla schedule 4 life forever start-time now
D2(config)# ip sla 6
D2(config-ip-sla) icmp-echo 2001:db8:100:1010::1
D2(config-ip-sla-echo)frequency 5
D2(config-ip-sla-echo)# exit
D2(config)# ip sla schedule 6 life forever start-time now
```

#### 4.3 En D1 configure HSRPv2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.

```
D1(config)#interface Vlan100
```

```
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
```

- Establezca la prioridad del grupo en 150.  
D1(config-if)#standby 104 priority 150
- Habilite la preferencia (preemption).  
D1(config-if)#standby 104 preempt
- Rastree el objeto 4 y decremente en 60.  
D1(config-if)#standby 104 track 4 decrement 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.  
D1(config)#interface Vlan101  
D1(config-if)#standby version 2  
D1(config-if)#standby 114 ip 10.0.101.254
- Habilite la preferencia (preemption).  
D1(config-if)#standby 114 preempt
- Rastree el objeto 4 para disminuir en 60.  
D1(config-if)#standby 114 track 4 decrement 60

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.  
D1(config)#interface Vlan102  
D1(config-if)#standby version 2  
D1(config-if)#standby 124 ip 10.0.102.254

- Establezca la prioridad del grupo en 150.  
D1(config-if)#standby 124 priority 150
- Habilite la preferencia (preemption).  
D1(config-if)#standby 124 preempt
- Rastree el objeto 4 para disminuir en 60.  
D1(config-if)#standby 124 track 4 decrement 60

Configure IPv6 HSRP grupo 106 para la VLAN 100

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D1(config-if)#standby 106 ipv6 autoconfig
- Establezca la prioridad del grupo en 150.  
D1(config-if)#standby 106 priority 150
- Habilite la preferencia (preemption).  
D1(config-if)#standby 106 preempt
- Rastree el objeto 6 y decremente en 60.  
D1(config-if)#standby 106 track 6 decrement 60

Configure IPv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D1(config-if)#standby 116 ipv6 autoconfig
- Habilite la preferencia (preemption).  
D1(config-if)#standby 116 preempt

- Registre el objeto 6 y decremente en 60.  
D1(config-if)#standby 116 track 6 decrement 60

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D1(config-if)#standby 126 ipv6 autoconfig
- Establezca la prioridad del grupo en 150.  
D1(config-if)#standby 126 priority 150
- Habilite la preferencia (preemption).  
D1(config-if)#standby 126 preempt
- Rastree el objeto 6 y decremente en 60.  
D1(config-if)#standby 126 track 6 decrement 60

En D2, configure HSRPv2.

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.  
D2(config)#interface Vlan100  
D2(config-if)#standby version 2  
D2(config-if)#standby 104 ip 10.0.100.254
- Habilite la preferencia (preemption).  
D2(config-if)#standby 104 preempt

- Rastree el objeto 4 y decremente en 60.  
D2(config-if)#standby 104 track 4 decrement 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.  
D2(config)#interface Vlan101  
D2(config-if)#standby version 2  
D2(config-if)#standby 114 ip 10.0.101.254
- Establezca la prioridad del grupo en 150.  
D2(config-if)#standby 114 priority 150
- Habilite la preferencia (preemption).  
D2(config-if)#standby 114 preempt
- Rastree el objeto 4 para disminuir en 60.  
D2(config-if)#standby 114 track 4 decrement 60

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.  
D2(config)#interface Vlan102  
D2(config-if)#standby version 2  
D2(config-if)#standby 124 ip 10.0.102.254
- Habilite la preferencia (preemption).  
D2(config-if)#standby 124 preempt
- Rastree el objeto 4 para disminuir en 60.  
D2(config-if)#standby 124 track 4 decrement 60



Configure IPv6 HSRP grupo 106 para la VLAN 100:

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D2(config-if)#standby 106 ipv6 autoconfig
- Habilite la preferencia (preemption).  
D2(config-if)#standby 106 preempt
- Rastree el objeto 6 para disminuir en 60.  
D2(config-if)#standby 106 track 6 decrement 60

Configure IPv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D2(config-if)#standby 116 ipv6 autoconfig
- Establezca la prioridad del grupo en 150.  
D2(config-if)#standby 116 priority 150
- Habilite la preferencia (preemption).  
D2(config-if)#standby 116 preempt
- Rastree el objeto 6 para disminuir en 60.  
D2(config-if)#standby 116 track 6 decrement 60

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando ipv6 autoconfig.  
D2(config-if)#standby 126 ipv6 autoconfig
- Habilite la preferencia (preemption).  
D2(config-if)#standby 126 preempt

- Rastree el objeto 6 para disminuir en 60.  
D2(config-if)#standby 126 track 6 decrement 60

## Parte 5: Seguridad

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

- **D1**  
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
- **D2**  
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
- **R1**  
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
- **R2**  
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
- **R3**  
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
- **A1**  
A1(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.

- **D1.**  
D1(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco
- **D2.**  
D2(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco

- **R1.**  
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco
- **R2.**  
R2(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco
- **R3.**  
R3(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco
- **A1.**  
A1(config)#username sadmin privilege 15 algorithm-type SCRYPT  
secret cisco12345cisco

### 5.3 En todos los dispositivos (Excepto R2), habilite AAA

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

```
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
acct-port 1813
D1(config-radius-server)#key $strongPass
```

```
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
acct-port 1813
D2(config-radius-server)#key $strongPass
```

```
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
acct-port 1813
R1(config-radius-server)#key $strongPass
```

```
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
acct-port 1813
R3(config-radius-server)#key $strongPass
```

```
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812
acct-port 1813
A1(config-radius-server)#key $strongPass
```

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

Use la lista de métodos por defecto

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

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

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

```
R3(config)#aaa authentication login default group radius local
```

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

#### 5.6 Verifique el servicio AAA en todos los dispositivos (except R2)

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

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

#### 6.1 Configure R2 como un NTP maestro.

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

```
D2(config)#ntp master 3
```

#### 6.2 Configure NTP en R1, R3, D1, D2, y A1

Configure NTP de la siguiente manera:

- R1 debe sincronizar con R2

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

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

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

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

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

- D2 para sincronizar la hora con R3.

```
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.

```
R1(config)# logging trap warning
```

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

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

```
R1(config)#ip access-list standard SNMP-NMS
```

```
R1(config-std-nacl)# permit host 10.0.100.5
```

```
R3(config)# logging trap warning
```

```
R3(config)# logging host 10.0.100.5
```

```
R3(config)# logging on
```

```
R3(config)#ip access-list standard SNMP-NMS
```

```
R3(config-std-nacl)# permit host 10.0.100.5
```

```
D1(config)# logging trap warning
```

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

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

```
D1(config)#ip access-list standard SNMP-NMS
```

```
D1(config-std-nacl)# permit host 10.0.100.5
```

```
D2(config)# logging trap warning
```

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

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

```
D2(config)#ip access-list standard SNMP-NMS
```

```
D2(config-std-nacl)# permit host 10.0.100.5
```

```
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)# permit host 10.0.100.5
```

## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

- Limite el acceso SNMP a la dirección IP de la PC1.  
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
- Configure el valor de contacto SNMP con su nombre.  
D2(config)# snmp-server contact LEYDI MARCELA
- Establezca el community string en ENCORSA.  
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
- En R3, D1, y D2, habilite el envío de traps config y ospf.  
R3(config)# snmp-server ifindex persist  
R3(config)# snmp-server enable traps config  
R3(config)# snmp-server enable traps ospf  
  
D1(config)# snmp-server ifindex persist  
D1(config)# snmp-server enable traps config  
D1(config)# snmp-server enable traps ospf  
  
D2(config)# snmp-server ifindex persist

```
D2(config)# snmp-server enable traps config
```

```
D2(config)# snmp-server enable traps ospf
```

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

```
R1(config)# snmp-server ifindex persist
```

```
R1(config)# snmp-server enable traps bgp
```

```
R1(config)# snmp-server enable traps config
```

```
R1(config)# snmp-server enable traps ospf
```

- En A1, habilite el envío de traps config.

```
A1(config)# snmp-server ifindex persist
```

```
A1(config)# snmp-server enable traps config
```

```
A1(config)# snmp-server enable traps ospf
```



## CONCLUSIONES

En el transcurso del Diplomado se fueron realizando laboratorios en cada una de las fases en donde se logró practicar a partir de simulaciones en la plataforma Packet Tracer y el GNS3, llevando al estudiante a una adquisición bastante crítica de los conocimientos aprendidos en el área de las telecomunicaciones. Es así, como el Diplomado de Profundización CCNP, no solo prepara al estudiante en conocimientos teóricos, sino que lo lleva a la destreza de habilidades y aptitudes prácticas, planificando, implementando, manteniendo y aportando soluciones a problemas de redes convergentes en las diferentes economías existentes. Realmente el Diplomado es una plataforma que lleva al estudiante a poder desenvolverse en el área de Redes, de Sistemas, como asesor, integrador y administrador de redes.

Durante el desarrollo del escenario sugerido se logró la practica los temas de la unidad 1 del curso de enrutamiento OSPF, implementar protocolos y establecer los protocolos de conexión estos mismos de acuerdo con sus respectivas características lo cual sin duda tiene sus propias ventajas.

Al finalizar este proyecto propuesto por el grupo de docentes de la UNAD, se logra configurar y gestionar módulos de Networking en redes escalables, ofreciendo seguridad y confianza en las redes. El escenario planteado lleva a que se comprueben que los equipos cisco si otorgan la información y datos requeridos en cada uno de los ejercicios.

La correcta configuración entre la VLAN con VTP ofrece la posibilidad de independizar áreas de trabajo dentro de una empresa. Al identificar los protocolos de enrutamiento, se ayuda a proporcionar mejores tiempos de convergencia, extremadamente rápidos con un tráfico de red reducido.

## BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Disponible en: <https://1drv.ms/b/s!AmIJYeiNT1InMfy2rhPZHwEoWx>

UNAD (2015). Switch CISCO -Procedimientos de instalación y configuración del IOS [OVA]. Disponible en: <https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Disponible en: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>