

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**RAQUEL SOFIA GALLO GALINDO**

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

**DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

**RAQUEL SOFIA GALLO GALINDO**

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

**DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA**

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

**2021**

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

\_\_\_\_\_  
Firma del presidente del Jurado

\_\_\_\_\_  
Firma del Jurado

\_\_\_\_\_  
Firma del Jurado

BOGOTA, 27 de noviembre 2021

## AGRADECIMIENTOS

Agradezco primero que todo a mi familia y mi alma mater la UNAD que me ha dado tanto a nivel profesional y personal, a mejorado mi vida en presente y a futuro

## CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS.....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN.....	10
DESARROLLO .....	11
1. Escenario 1 .....	11
CONCLUSIONES .....	45
BIBLIOGRAFÍA.....	46

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	13
--	----

## LISTA DE FIGURAS

Figura 1. Escenario 1 -----	11
Figura 2. Simulación de escenario 1-----	12
Figura 3. Direccionamiento PC 1-----	23
Figura 4. direccionamiento PC 4 -----	23
Figura 5. Verificación servicios DHCP en PC2 -----	29
Figura 6. Verificación los servicios DHCP en PC3 -----	29
Figura 7. Verificación conectividad LAN en PC1 -----	30
Figura 8. Verificación conectividad LAN en PC2-----	30
Figura 9. Verificación conectividad LAN en PC3-----	31
Figura 10. Verificación conectividad LAN en PC4 -----	31
Figura 11. Verificación servicio AAA en PC4 -----	40
Figura 12. Configuración Syslog en PC1-----	42

## GLOSARIO

OSPF (*Open Shortest Path First*) protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP)

VTP (VLAN Trunking Protocol), protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

NAT (Network Address Translator), mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados

HSRP (*Hot Standby Router Protocol*) protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos (*single point of failure*) en la red mediante técnicas de redundancia y comprobación del estado de los routers.

GRE (*Generic Routing Encapsulation*) protocolo para el establecimiento de túneles a través de Internet. Está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar hasta 20 protocolos del nivel de red (nivel 3 del modelo OSI) distintos



## RESUMEN

Este documento contiene la prueba habilidades del curso, DIPLOMADO DE PROFUNDIZACION CISCO CCNP, el cual consta de 6 partes las cuales se dividen en dos escenarios y se realizan en dos entregas

El primer escenario propone, la configuración de una red en la cual se realiza un enrutamiento, con el objetivo de comunicar un extremo con el otro, que los protocolos implementados sean operativos dentro de la red de la compañía, por medio de dispositivos CISCO especializados en la conmutación y enrutamiento de paquetes

El segundo escenario comprende la parte de autenticación, listas de control de acceso (ACL), HSRP versión 2 para brindar redundancia a los hosts, configuración de mecanismos de seguridad para las redes y sus dispositivos, configuración de horario en los hosts, etc.

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

## ABSTRACT

This document contains the skills test of the course, CISCO CCNP DEEPENING DIPLOMA, which consists of 6 parts which are divided into two scenarios and are carried out in two deliveries

The first scenario proposes, the configuration of a network in which a routing is carried out, in order to communicate one end with the other, that the implemented protocols are operative within the company network, by means of CISCO devices specialized in packet switching and routing

The second scenario comprises the authentication part, access control lists (ACLs), HSRP version 2 to provide redundancy to the hosts, configuration of security mechanisms for the networks and their devices, configuration of the schedule in the hosts, etc.

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

## INTRODUCCIÓN

El DIPLOMADO DE PROFUNDIZACION CISCO CCNP, es una valiosa herramienta que brinda a los profesionales del área de las telecomunicaciones, entornos de prueba para poner en marcha nuevas implementaciones a nivel de networking, evitando y controlando fallas en las redes que se pueden presentar en real time, afectando la operación de compañías y clientes

El primer escenario que se propuso fue, la configuración de una red en la cual se realiza un enrutamiento, con el objetivo de comunicar un extremo con el otro, que los protocolos implementados sean operativos dentro de la red de la compañía, por medio de dispositivos CISCO especializados en la conmutación y enrutamiento de paquetes

El segundo escenario comprende la parte de autenticación, listas de control de acceso (ACL), HSRP versión 2 para brindar redundancia a los hosts, configuración de mecanismos de seguridad para las redes y sus dispositivos, configuración de horario en los hosts, etc.

# DESARROLLO

## 1. ESCENARIO 1

Figura 1. Escenario 1

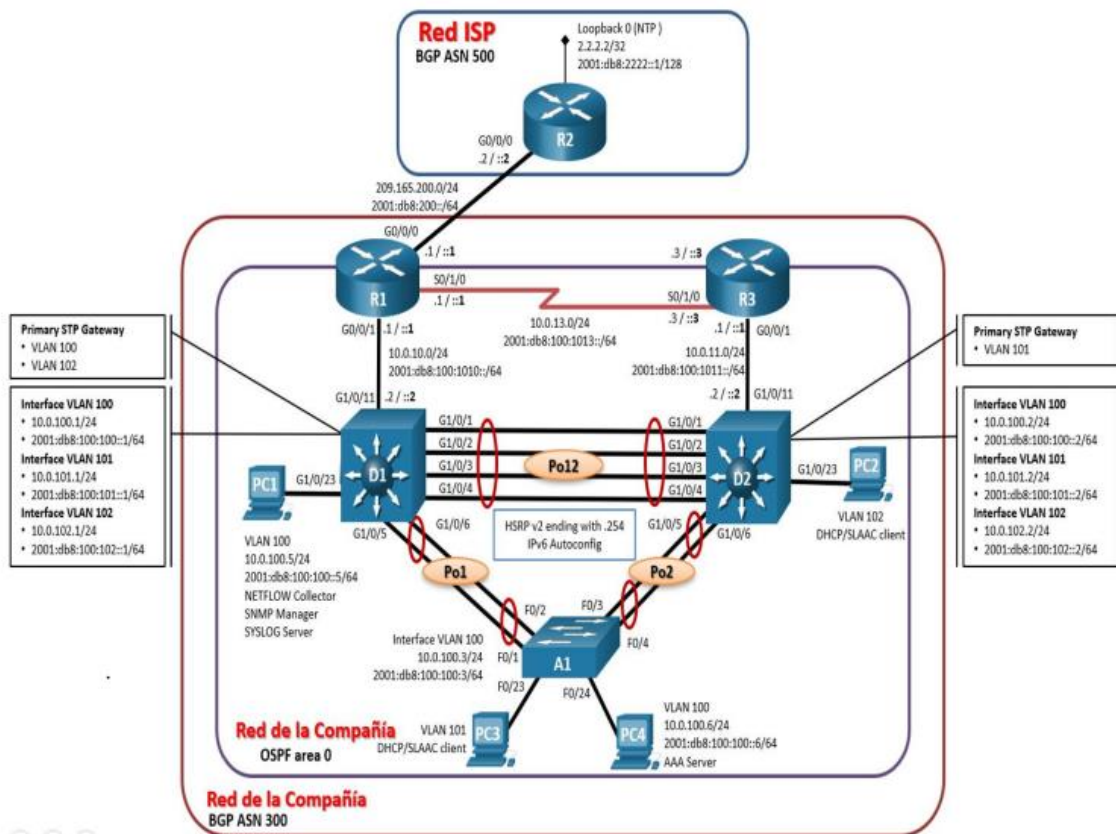


Figura 2. Simulación de escenario 1

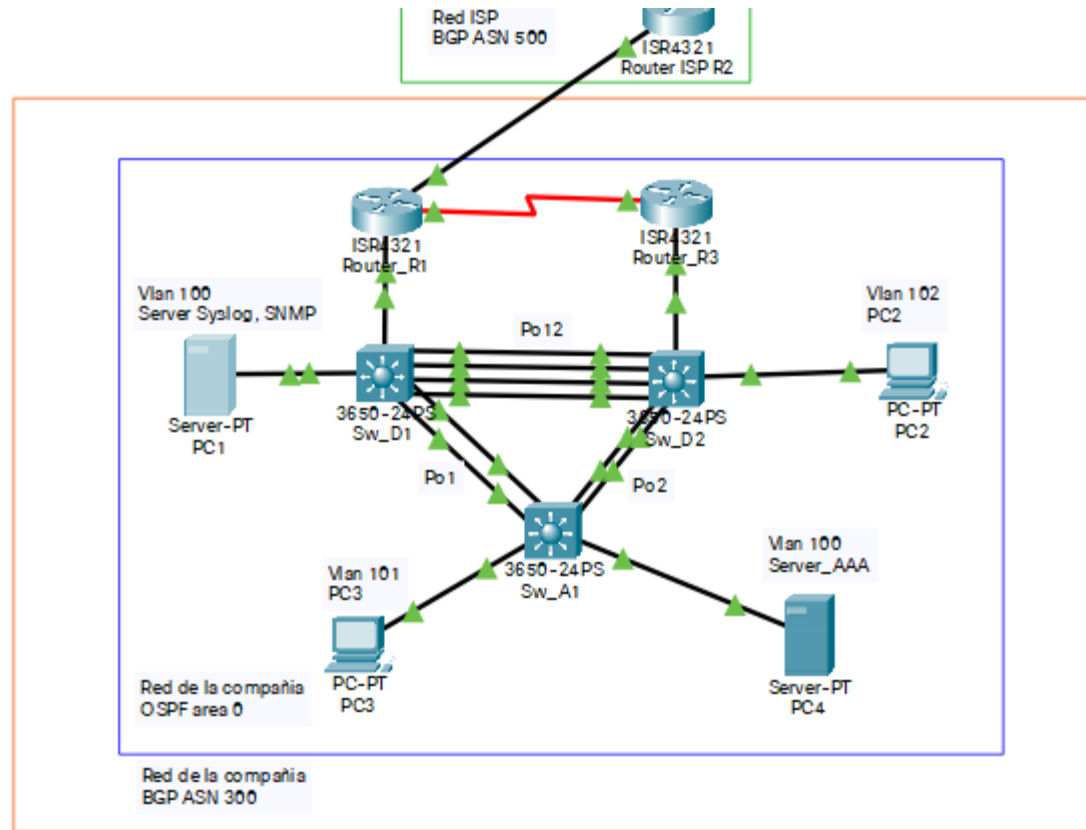


Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

## **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.

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

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

a. 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**

```
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 g0/0/0
```

```
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 g0/0/1
```

```
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 s0/1/0
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
```

### **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

```
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

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, g1/0/12-24, g1/1/1-4

shutdown

exit
```

## **witch 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, g1/0/12-24, 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
```

```
lan 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
```

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

D1#copy running-config startup-config

**c. 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 3. direccionamiento PC 1

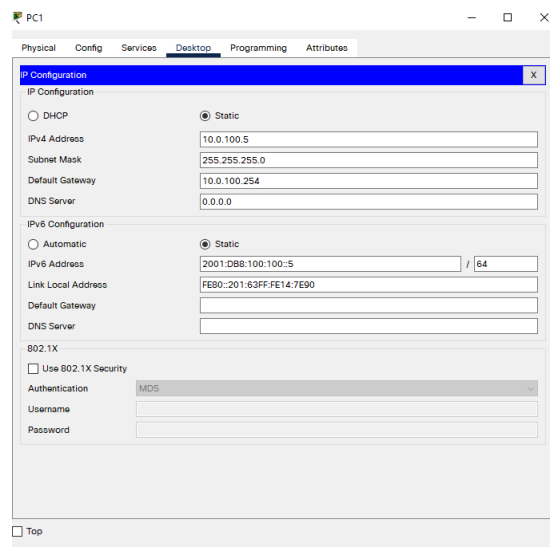
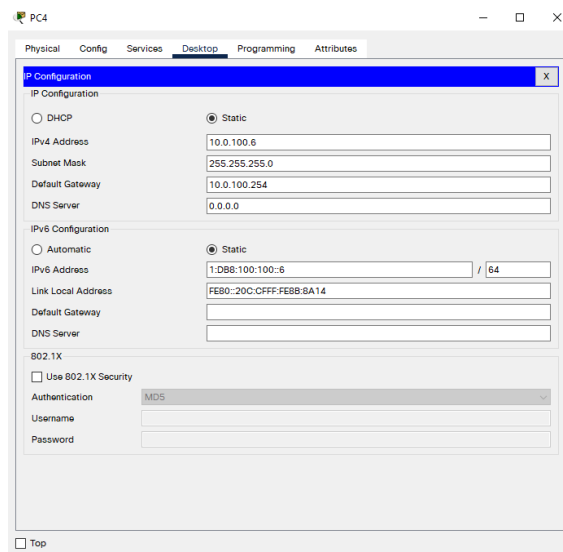


Figura 4. direccionamiento PC 4



## 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.

Las tareas de configuración son las siguientes:

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

### SW D1 a SW D2 / SW A1

```
interface Port-channel1
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface Port-channel12
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 12 mode active
!
interface GigabitEthernet1/0/2
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 12 mode active
!
interface GigabitEthernet1/0/3
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 12 mode active
```



```
interface GigabitEthernet1/0/4
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 12 mode active
```

```
interface GigabitEthernet1/0/5
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
```

```
!
interface GigabitEthernet1/0/6
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
```

D2 a A1 se configuro de igual manera

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

### **SW D1**

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
!
interface GigabitEthernet1/0/2
switchport trunk native vlan 999
!
interface GigabitEthernet1/0/3
switchport trunk native vlan 999
!
interface GigabitEthernet1/0/4
switchport trunk native vlan 999
```

```
interface GigabitEthernet1/0/5
switchport trunk native vlan 999
!
interface GigabitEthernet1/0/6
switchport trunk native vlan 999
```

D2 se configure de igual manera

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

SW D1: spanning-tree mode rapid-pvst

SW D2: spanning-tree mode rapid-pvst

SW A1: 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).**

SW D1: spanning-tree vlan 100,102 priority 24576

```
interface Vlan100
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
ipv6 ospf 6 area 0
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
```

```
interface Vlan101
mac-address 0006.2a3b.0702
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
ipv6 ospf 6 area 0
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 116 ipv6 autoconfig
standby 116 preempt
```

```
!
interface Vlan102
mac-address 0006.2a3b.0703
ip address 10.0.102.1 255.255.255.0
ipv6 address FE80::D1:4 link-local
standby 126 preempt
```

```
ipv6 address 2001:DB8:100:102::1/64
ipv6 ospf 6 area 0
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 126 ipv6 autoconfig
standby 126 priority 150
```

**SW D2:** spanning-tree vlan 101 priority 24576

```
interface Vlan101
mac-address 000a.f3b5.9903
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
ipv6 ospf 6 area 0
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
```

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

**SW D1 a D2 / A1**

```
interface Port-channel1
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface Port-channel12
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
```

## **SW D2 a SW A1**

```
interface Port-channel2
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface Port-channel12
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
```

**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.**

## **SW D1**

```
interface GigabitEthernet1/0/23
switchport access vlan 100
switchport mode Access
switchport nonegotiate
```

## **SW D2**

```
interface GigabitEthernet1/0/23
switchport access vlan 102
switchport mode access
switchport nonegotiate
```

## **SW A1**

```
interface GigabitEthernet1/0/23
switchport access vlan 101
switchport mode Access
switchport nonegotiate
```

## 2.7 Verifique los servicios DHCP IPv4

Figura 5. Verificación servicios DHCP en PC2

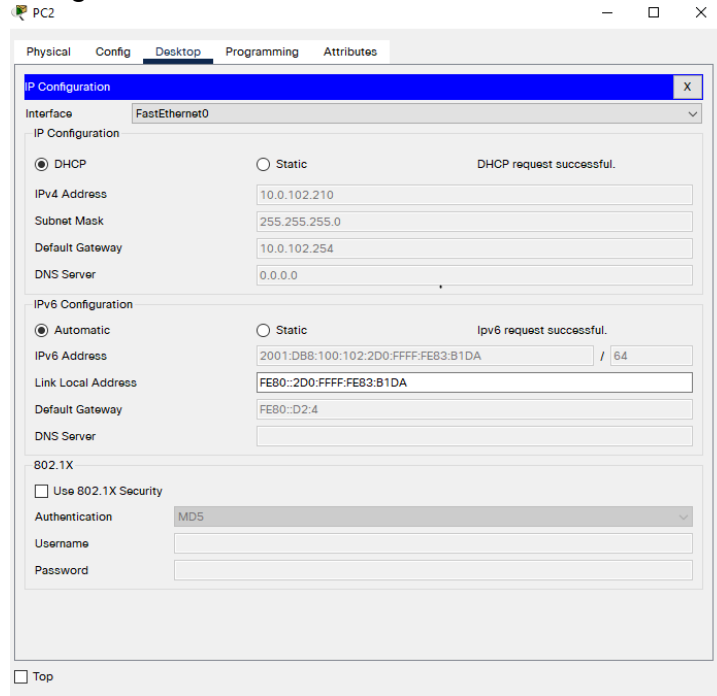
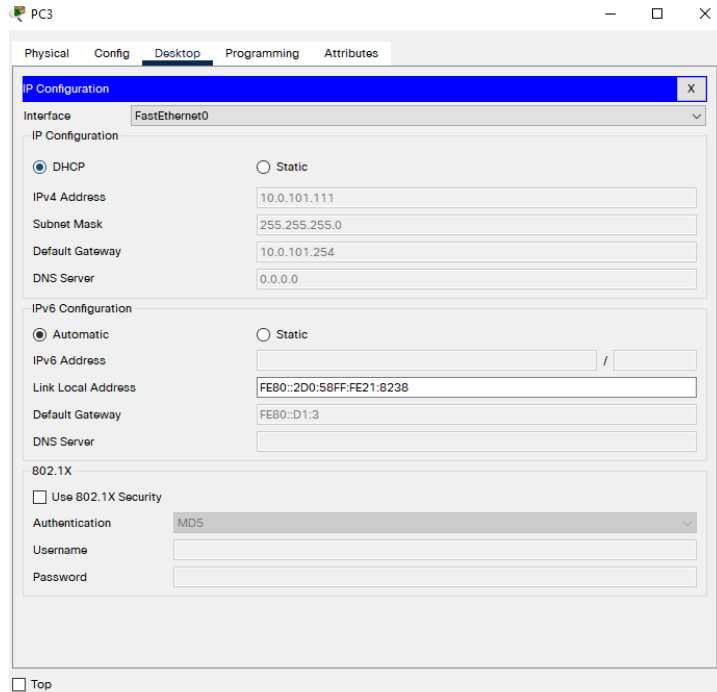
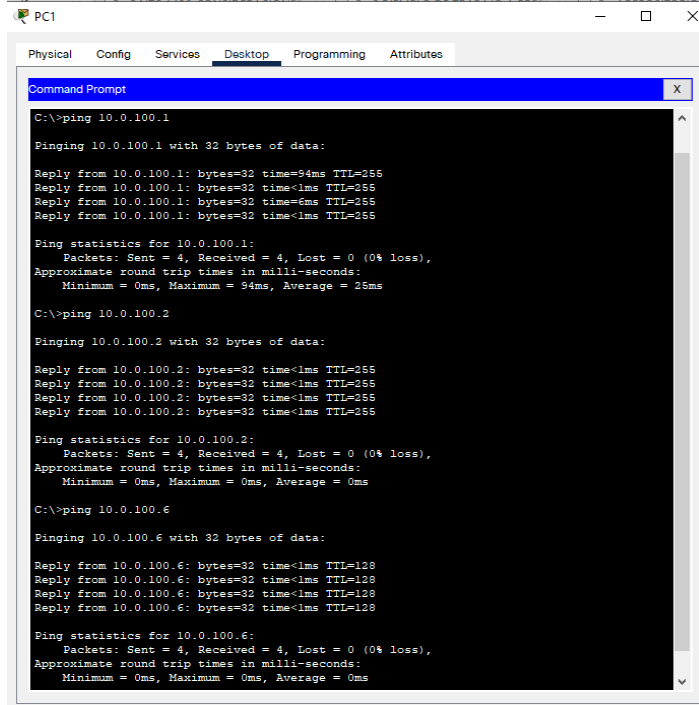


Figura 6. Verificación los servicios DHCP en PC3



## 2.8 Verifique la conectividad de la LAN local

Figura 7. Verificación conectividad LAN en PC1



```
PC1
Physical Config Services 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=94ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time=6ms 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 = 94ms, Average = 28ms

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

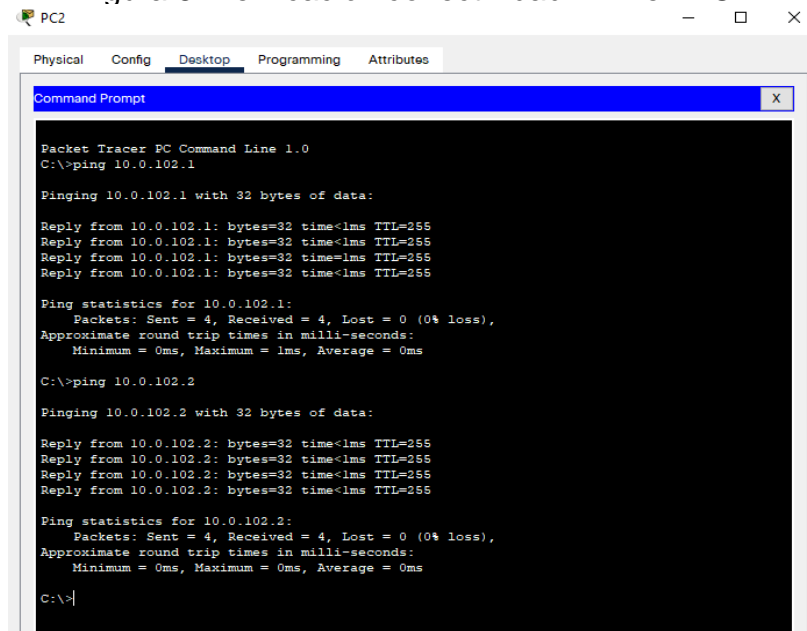
Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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 8. Verificación conectividad LAN en PC2



```
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<1ms TTL=255
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<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 = 1ms, Average = 0ms

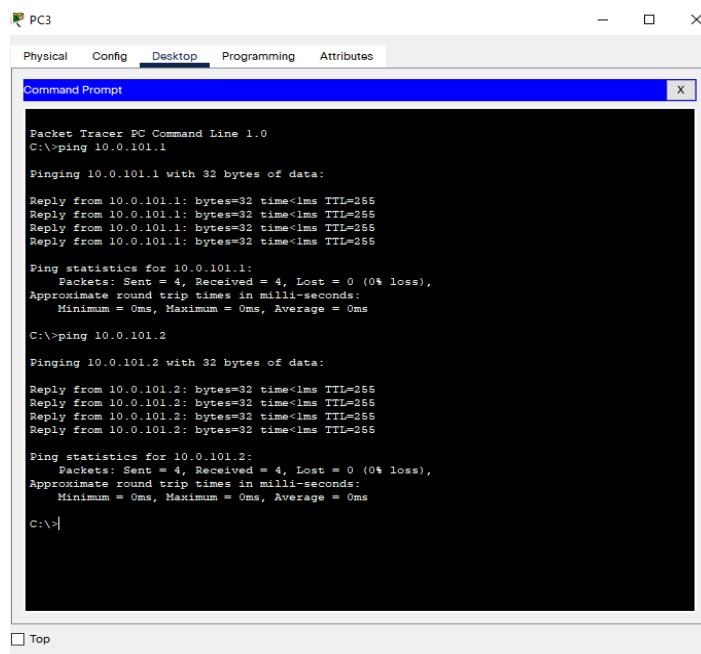
C:\>ping 10.0.102.2
Pinging 10.0.102.2 with 32 bytes of data:

Reply from 10.0.102.2: bytes=32 time<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:\>
```

Figura 9. Verificación conectividad LAN en PC3



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

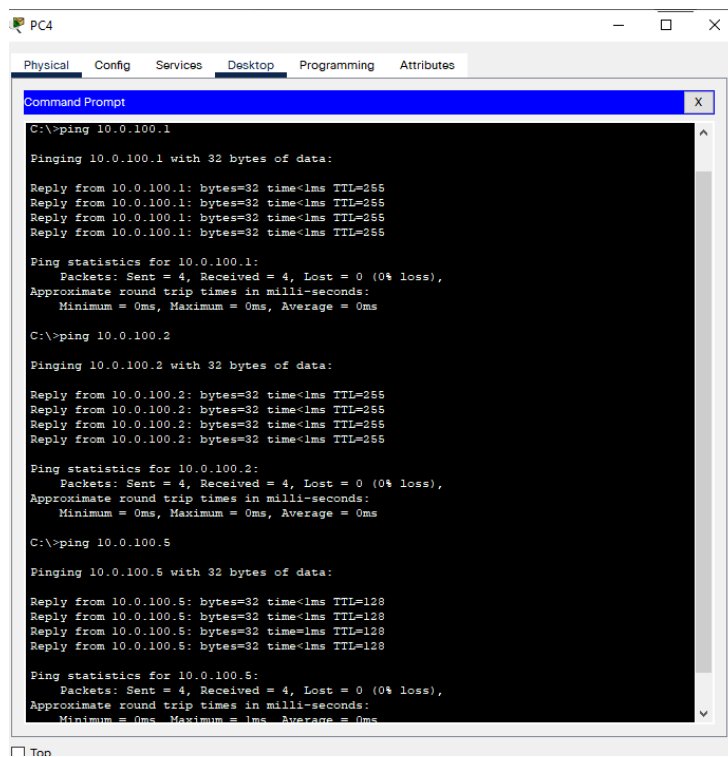
Pinging 10.0.101.2 with 32 bytes of data:

Reply from 10.0.101.2: bytes=32 time<ms TTL=255
Reply from 10.0.101.2: bytes=32 time<ms TTL=255
Reply from 10.0.101.2: bytes=32 time<ms TTL=255
Reply from 10.0.101.2: bytes=32 time<ms 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:\>|
```

Figura 10. Verificación conectividad LAN en PC4



```
PC4
Physical Config Services 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<ms TTL=255
Reply from 10.0.100.1: bytes=32 time<ms TTL=255
Reply from 10.0.100.1: bytes=32 time<ms TTL=255
Reply from 10.0.100.1: bytes=32 time<ms 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<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms 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 10.0.100.5

Pinging 10.0.100.5 with 32 bytes of data:

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

## Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la

dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

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

### R1

```
router ospf 4
router-id 0.0.4.1
log-adjacency-changes
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

### R3

```
router ospf 4
router-id 0.0.4.3
log-adjacency-changes
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

### SW D1

```
router ospf 4
router-id 0.0.4.131
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet1/0/11
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
```



## SW D2

```
router ospf 4
router-id 0.0.4.132
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet1/0/11
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 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.**

## R1

```
router ospf 6
router-id 0.0.6.1
log-adjacency-changes

interface GigabitEthernet0/0/1
ip address 10.0.10.1 255.255.255.0
ipv6 ospf 6 area 0

interface Serial0/1/0
ip address 10.0.13.1 255.255.255.0
ipv6 ospf 6 area 0
```

## R3

```
router ospf 6
router-id 0.0.6.3
log-adjacency-changes

interface GigabitEthernet0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 ospf 6 area 0
!
interface Serial0/1/0
ip address 10.0.13.3 255.255.255.0
ipv6 ospf 6 area 0
```

## SW D1

```
router ospf 6
router-id 0.0.6.131
log-adjacency-changes
passive-interface Vlan100
passive-interface Vlan101
passive-interface Vlan102

interface GigabitEthernet1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 ospf 6 area 0
```

## SW D2

```
router ospf 4
router-id 0.0.4.132
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet1/0/11
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0

interface GigabitEthernet1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 ospf 6 area 0
```

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

#### R2

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
ipv6 address FE80::2:3 link-local
ipv6 address 2001:DB8:2222::1/128

ip classless
ip route 2.2.2.2 255.255.255.255 209.165.200.225
ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

```
ipv6 route 2001:DB8:2222::1/128 2001:DB8:200::1
```

```
router bgp 500  
bgp log-neighbor-changes  
no synchronization  
neighbor 209.165.200.225 remote-as 300  
network 2.2.2.2 mask 255.255.255.255  
redistribute static
```

#### COMANDOS NO SOPORTADOS POR PACKET TRACERT

En IPv4 address family, anuncie:

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

En IPv6 address family, anuncie:

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

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

#### R1

```
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.200.226  
ip route 10.0.0.0 255.0.0.0 Null0
```

```
ipv6 route ::/0 2001:DB8:200::2
```

```
router bgp 300  
bgp router-id 1.1.1.1  
bgp log-neighbor-changes  
no synchronization  
neighbor 209.165.200.226 remote-as 500  
network 10.0.0.0
```

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

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

No soportado por packet tracert

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

No soportado por packet tracert

### **4.3 En D1 configure HSRPv2.**

```
interface Vlan100
mac-address 0006.2a3b.0701
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
ipv6 ospf 6 area 0
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
```

```

interface Vlan101
mac-address 0006.2a3b.0702
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
ipv6 ospf 6 area 0
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 116 ipv6 autoconfig
standby 116 preempt
!
interface Vlan102
mac-address 0006.2a3b.0703
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
ipv6 ospf 6 area 0
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt

```

### **En D2 configure HSRPv2.**

```

interface Vlan100
mac-address 000a.f3b5.9901
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
ipv6 ospf 6 area 0
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 106 ipv6 autoconfig
standby 106 preempt

```

```
interface Vlan101
mac-address 000a.f3b5.9903
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
ipv6 ospf 6 area 0
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
```

```
interface Vlan102
mac-address 000a.f3b5.9904
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
ipv6 ospf 6 area 0
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 126 ipv6 autoconfig
standby 126 preempt
```

## Parte 5: Seguridad

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

Las tareas de configuración son las siguientes:

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

```
enable secret 5 $1$mERr$h/D.Fyei.K.4QxM5QhZ1i/  
D1(config)#enable secret cisco12345cisco
```

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

```
username sadmin privilege 15 password 7 0822455D0A165445415F590723382727
```

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

```
aaa new-model
```

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

```
radius server RADIUS  
address ipv4 10.0.100.6 auth-port 1812  
key $strongPass
```

Se configura de la misma forma en los demás dispositivos de la red menos R2

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

```
aaa authentication login AUT-RADIUS group radius local
```

```
logging synchronous  
login authentication AUT-RADIUS
```

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

Figura 11. verificación servicio AAA en PC4

The screenshot displays the configuration page for the AAA service on a device labeled PC4. The interface includes a sidebar menu with various services, a main configuration area for AAA, and a 'User Setup' section.

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**AAA**

Service:  On  Off Radius Port:

**Network Configuration**

Client Name:  Client IP:

Secret:  ServerType:

Client Name	Client IP	Server Type	Key	
1 AUT-RADIUS	10.0.10.1	Radius	StrongPass	<input type="button" value="Add"/>
2 AUT-RADIUS	10.0.11.1	Radius	StrongPass	<input type="button" value="Save"/>
				<input type="button" value="Remove"/>

**User Setup**

Username:  Password:

Username	Password	
1 raduser	upass123	<input type="button" value="Add"/>
		<input type="button" value="Save"/>
		<input type="button" value="Remove"/>

Top



## Parte 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.

```
comando clock set 10:30:00 28 Nov 2021
```

### 6.2 Configure R2 como un NTP maestro.

```
ntp master 3  
  
address ref clock st when poll reach delay offset disp  
*~127.127.1.1 .LOCL. 2 22 64 377 0.00 0.00 0.48
```

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

#### R1

```
ntp server 209.165.200.226  
  
address ref clock st when poll reach delay offset disp  
*~209.165.200.226 127.127.1.1 3 5 16 377 0.00 0.00 0.12
```

#### R3

```
ntp server 10.0.13.1  
  
address ref clock st when poll reach delay offset disp  
*~10.0.13.1 209.165.200.226 4 3 16 377 2.00 0.00 0.12
```

#### SW D1

```
ntp server 10.0.10.1
```

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

address ref clock st when poll reach delay offset disp  
~10.0.10.1 209.165.200.226 17 5 16 370 0.00 0.00 0.36

## SW A1

ntp server 10.0.10.1

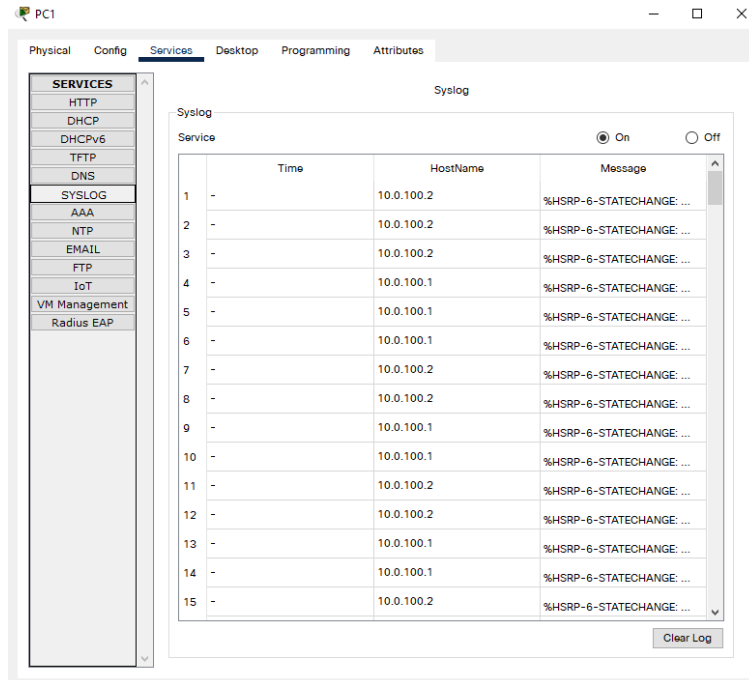
address ref clock st when poll reach delay offset disp  
~10.0.100.1 10.0.10.1 5 7 16 377 0.00 0.00 0.12

## SW D2

ntp server 10.0.11.1

address ref clock st when poll reach delay offset disp  
~10.0.11.1 10.0.13.1 5 19459 16 373 0.00 4.00 0.12

Figura 12. Configuración Syslog en PC1



## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2

```
logging 10.0.100.5
line con 0
exec-timeout 0 0
logging synchronous
D1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
```

No Active Message Discriminator.

No Inactive Message Discriminator.

```
Console logging: level debugging, 92 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 92 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled
```

```
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

se configura igual en todos los dispositivos excepto R2

## 6.5 Configure SNMPv2c en todos los dispositivos excepto R2

```
ip access-list standard SNMP-SERVER
permit host 10.0.100.5

snmp-server community ENCORSA RO
```

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

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

En A1, habilite el envío de traps config

Comando no reconocidos por packet tracer



## CONCLUSIONES

El implementar el escenario propuesto en el DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP, como profesional y estudiante fue una interesante prueba de conocimiento, habilidades, disciplina, paciencia, perseverancia y demás

Gracias a aplicativos creados por casa productoras de hardware y software para telecomunicaciones como CISCO, los estudiantes y profesionales logran desarrollar destrezas que en entornos de pruebas son difíciles de adquirir, es una gran herramienta, pues se practica y se aprende bajo sus parámetros, parámetros que son actualizados constantemente, aplicados en las telecomunicaciones y por ende en la vida profesional

Desarrollar el escenario propuesto en el DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP, ayuda a conocer a profundidad y definir al estudiante, cual parte de networkin es más de su agrado, le apasiona y se le facilita, pudiendo definir a futuro y con seguridad en que campo especializarse al culminar el pregrado

La UNAD como alma mater deja un gran bagaje al estudiante, como profesional y persona, gracias a la UNAD y la perseverancia, el amor, la convicción de los estudiantes se cumplen sueños, se culminan metas, y vamos por más.....

## BIBLIOGRÁFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced BGP. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Troubleshooting Wireless Connectivity. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>