

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRACTICAS CCNP

CINDY CAROLINA GONZALEZ

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

CINDY CAROLINA GONZALEZ

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

Lograr esto en mi formación profesional me hizo pensar que la dedicación y la disciplina lo pueden todo, en primer lugar, agradecer a Dios, a mis padres ya mi familia, de quienes recibí el mejor aliento y cumplí mi sueño. A partir de ahora, brindaré con orgullo el mejor servicio a la sociedad.

CONTENIDO

AGRADECIMIENTO	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	10
INTRODUCCION	11
ESCENARIO 1	12
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	12
Parte 2: Configurar la capa 2 de la red y el soporte de Host	22
Parte 3: Configurar los protocolos de enrutamiento	31
Parte 4: Configurar la Redundancia de Primer Salto(Fist Hop Redundancy)	40
Parte 5: Seguridad	47
Parte 6: Configure las funciones de Administración de Red	53
CONCLUSIONES	56
BIBLIOGRAFIA	57

LISTA DE TABLAS

TABLA 1 HOST PC 1.....	21
TABLA 2 HOST PC 4.....	22

LISTA DE FIGURAS

FIGURA 1 TOPOLOGÍA DE RED ESCENARIO 1	12
FIGURA 2 HOST PC 1	21
FIGURA 3 HOST PC 4	22
FIGURA 4 DHCP PC2	26
FIGURA 5 DHCP PC3	27
FIGURA 6 VERIFICACIÓN LAN PC1	28
FIGURA 7 PC2 PING D1: 10.0.102.1 D2: 10.0.102.2.....	29
FIGURA 8 PC3 PING D1: 10.0.101.1 D2: 10.0.101.2.....	30
FIGURA 9 PC4 PING D1: 10.0.100.1 D2: 10.0.100.2: PC1: 10.0.100.5.....	31
FIGURA 10 SESION RADIUS R1.....	50
FIGURA 11 SESION RADIUS R3.....	51
FIGURA 12 SESION RADIUS D1.....	52
FIGURA 13 SESION RADIUS A1	52

GLOSARIO

BGP: es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

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.

Interface loopback: una interfaz loopback es aquella interfaz virtual mas no física que sirve para tener latente el protocolo de enrutamiento como OSPF, el cual, al no detectar interfaces activas en el dispositivo después de cierto tiempo.

LACP: es un protocolo estándar de la industria que se utiliza para agrupar dos o más enlaces y puede funcionar con dispositivos de diferentes proveedores, los puertos del conmutador físico que ejecutan el protocolo LACP pueden estar en modo pasivo o activo.

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

RESUMEN

El siguiente trabajo desarrolla un escenario relacionado con diferentes aspectos de las redes de datos de la plataforma Cisco, y describe en detalle las distintas etapas de ejecución. Las capturas de pantalla apoyan este escenario. Esto se logra mediante la implementación del protocolo de mapeo de VLAN a través de la red específica. Interfaz el uso de equipos electrónicos.

El intercambio de señales de red desde la fuente hasta el destino deseado es una parte esencial de la interconexión de computadoras y dispositivos periféricos. Como parte básica de la interconexión entre computadoras y dispositivos periféricos, los dispositivos electrónicos se utilizan para intercambiar señales de red desde la fuente hasta el destino deseado. Aplicando comandos de configuración a diferentes tipos de dispositivos activos, se pueden recuperar los conocimientos previos.

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

ABSTRACT

The following paper develops a scenario related to different aspects of Cisco platform data networks and describes in detail the different stages of execution. The screenshots support this scenario. This is achieved by implementing the VLAN mapping protocol across the specific network. Interface the use of electronic equipment.

The exchange of network signals from the source to the desired destination is an essential part of the interconnection of computers and peripheral devices. As a basic part of the interconnection between computers and peripheral devices, electronic devices are used to exchange network signals from the source to the desired destination. By applying configuration commands to different types of active devices, previous knowledge can be retrieved.

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

INTRODUCCION

La prueba de habilidades prácticas es una herramienta de evaluación del Diplomado de profundización de CCNP, con la cual se busca medir las habilidades y competencias que el estudiante logró alcanzar mediante el desarrollo del diplomado y cada una de sus actividades, esta evaluación pondrá a prueba al estudiante mediante la solución de problemas relacionados con redes.

Para el desarrollo del escenario se utilizará el software de simulación GNS3 para el diseño de la topología y la configuración de cada uno de los dispositivos se realizará la configuración de protocolos en los routers.

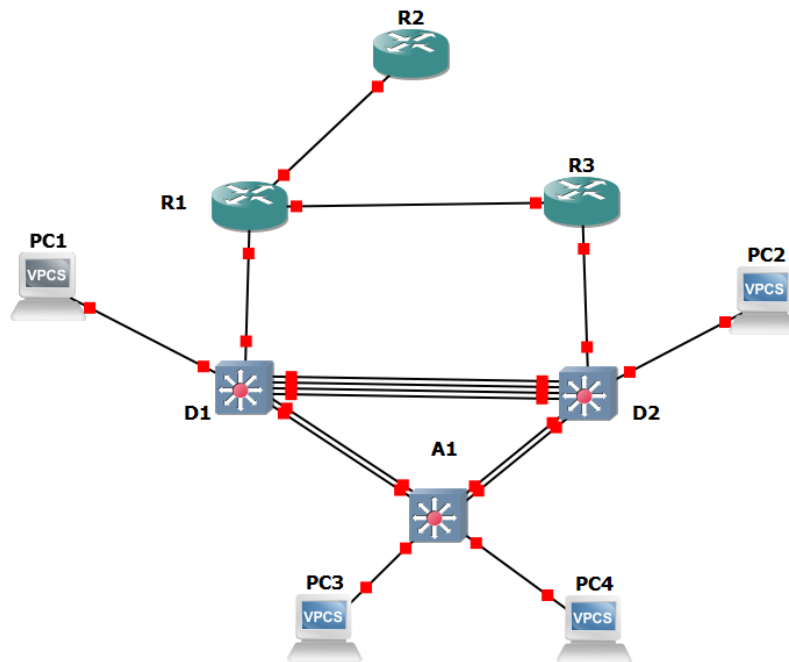
Se complementa la topología de red configurando e Interconectando los diferentes dispositivos realizando los diferentes lineamientos de direccionamiento, creación de puertos Etherchannel, creación de Vlan establecidas según el escenario y eligiendo servidor principal a través de la verificación y correcto funcionamiento de los componentes de las Vlan creadas de acuerdo con lo solicitado.

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 E0/0
  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 E0/1
  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 E2/0
  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 E0/0/0
  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 E0/1
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 E1/0
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 E0/1
  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 e0/1-3
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 E0/1
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 E0/1-3
shutdown
exit
interface range E0/1-8
shutdown
exit
interface range E1/1-4
shutdown
exit
```

Switch A1

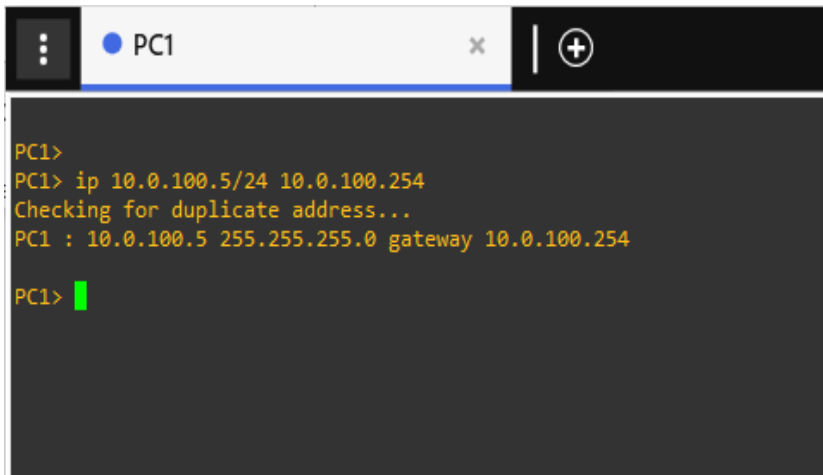
```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
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.

Tabla 1 host PC 1

Pc 1	
Ip	10.0.100.5
Mascara	255.255.255.0
Default gateway	10.0.100.254

Figura 2 host PC 1



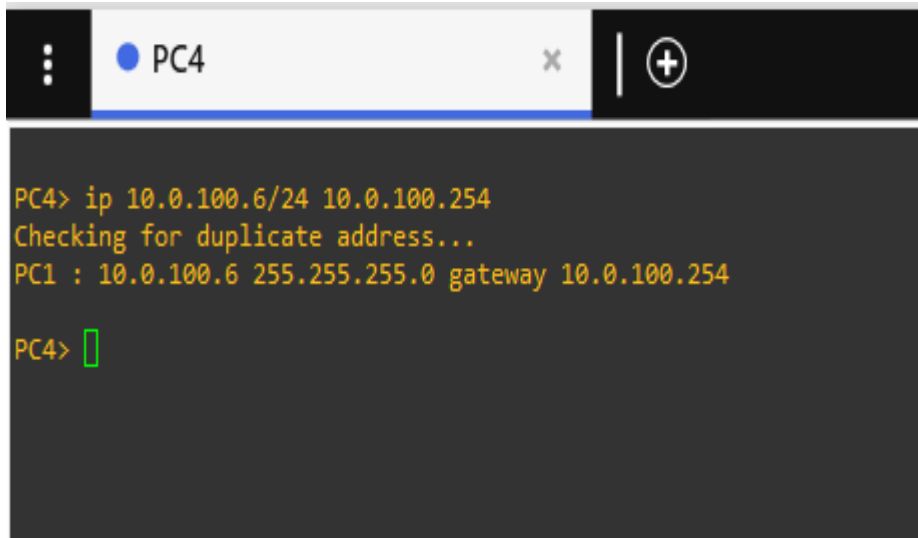
```
PC1>
PC1> ip 10.0.100.5/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> █
```

Tabla 2 host PC 4

Pc 4	
Ip	10.0.100.6
Mascara	255.255.255.0
Default gateway	10.0.100.254

Figura 3 host PC 4



```
PC4> ip 10.0.100.6/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC4> 
```

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 Ethernet 0/1 – 3
```

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

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

```
D2(config)#interface range Ethernet 0/1 - 3
```

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

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

```
A1(config)#interface range Ethernet 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 E0/1-3
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 E0/1-3
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 E1/1-2
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 E0/1-2
```

```
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 E1/0-2
```

```
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 E1/0-2
```

```
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 E1/3
```

```
D1(config-if)# switchport mode Access
```

```
D1(config-if)# switchport Access vlan 100
```

```
D1(config-if)# no shutdown
```

```
D2(config)# interface E1/3
```

```
D2(config-if)# switchport mode Access
```

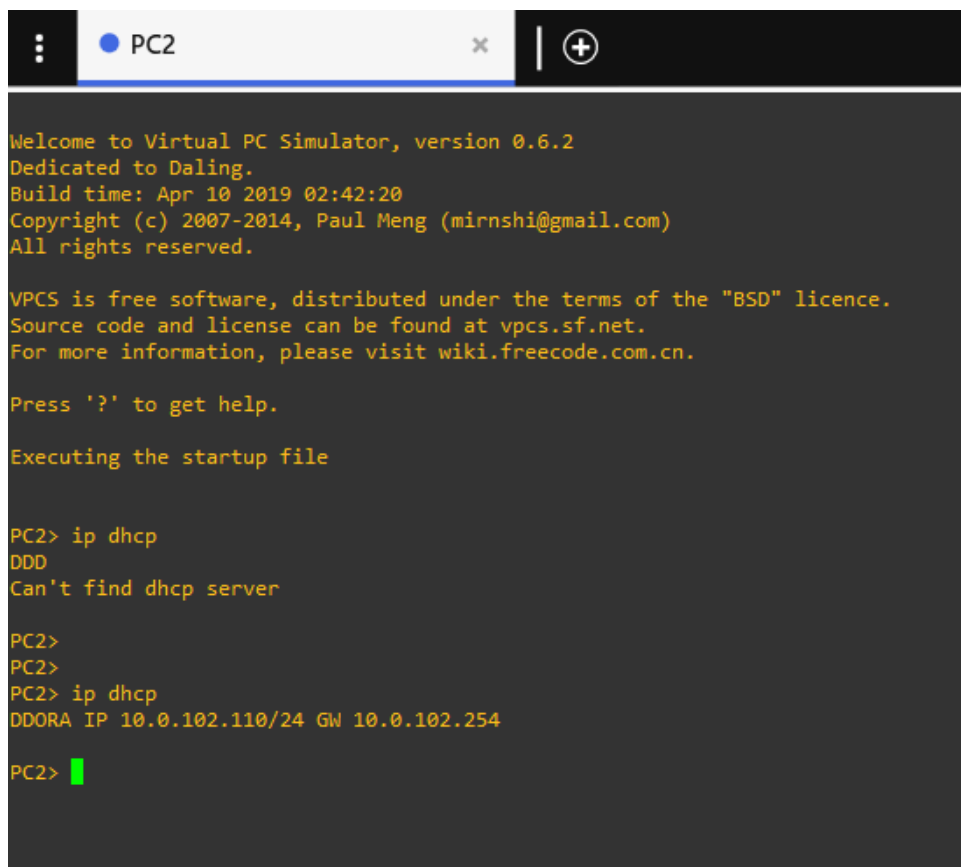
```
D2(config-if)# switchport Access vlan 102
```

```
D2(config-if)# no shutdown
```

```
A1(config)# interface E1/2
A1(config-if)# switchport mode Access
A1(config-if)# switchport Access vlan 101
A1(config-if)# no shutdown
A1(config)# interface E1/3
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



```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

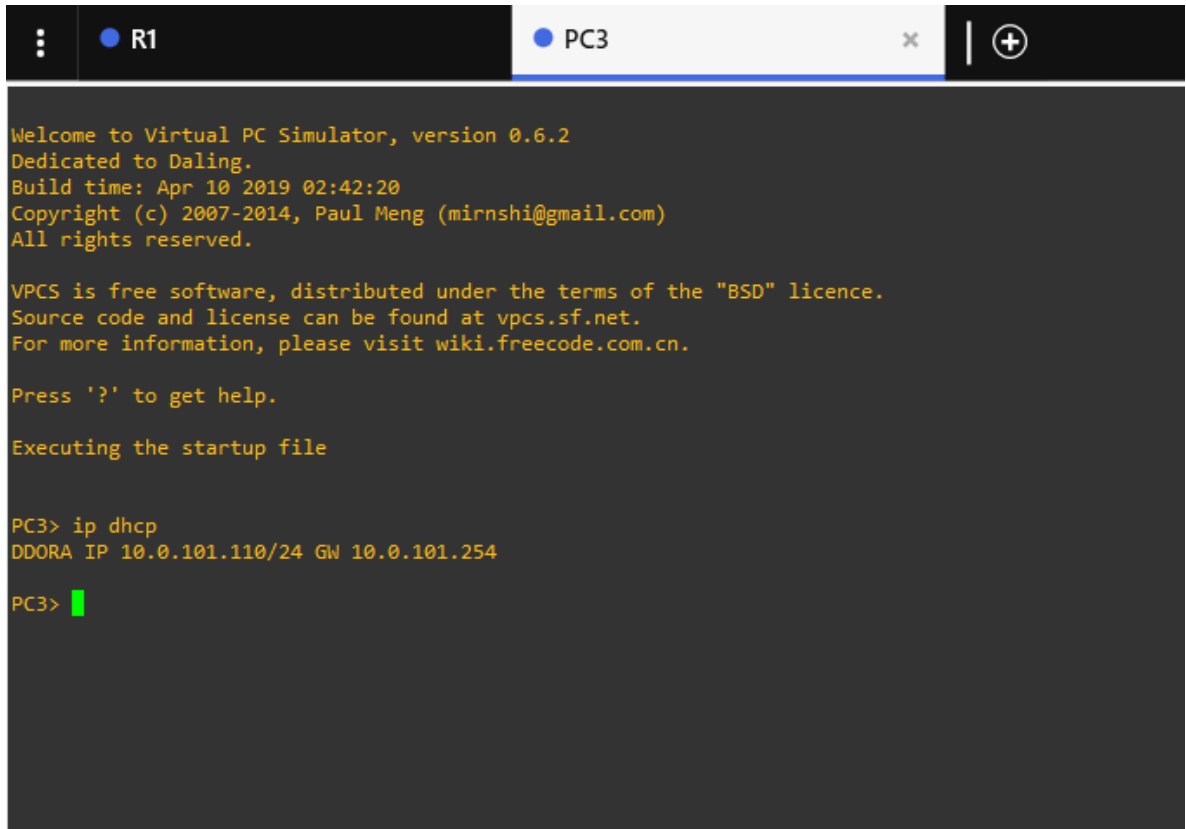
Executing the startup file

PC2> ip dhcp
DDD
Can't find dhcp server

PC2>
PC2>
PC2> ip dhcp
DDORA IP 10.0.102.110/24 GW 10.0.102.254

PC2> █
```

Figura 5 DHCP pc3



```
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

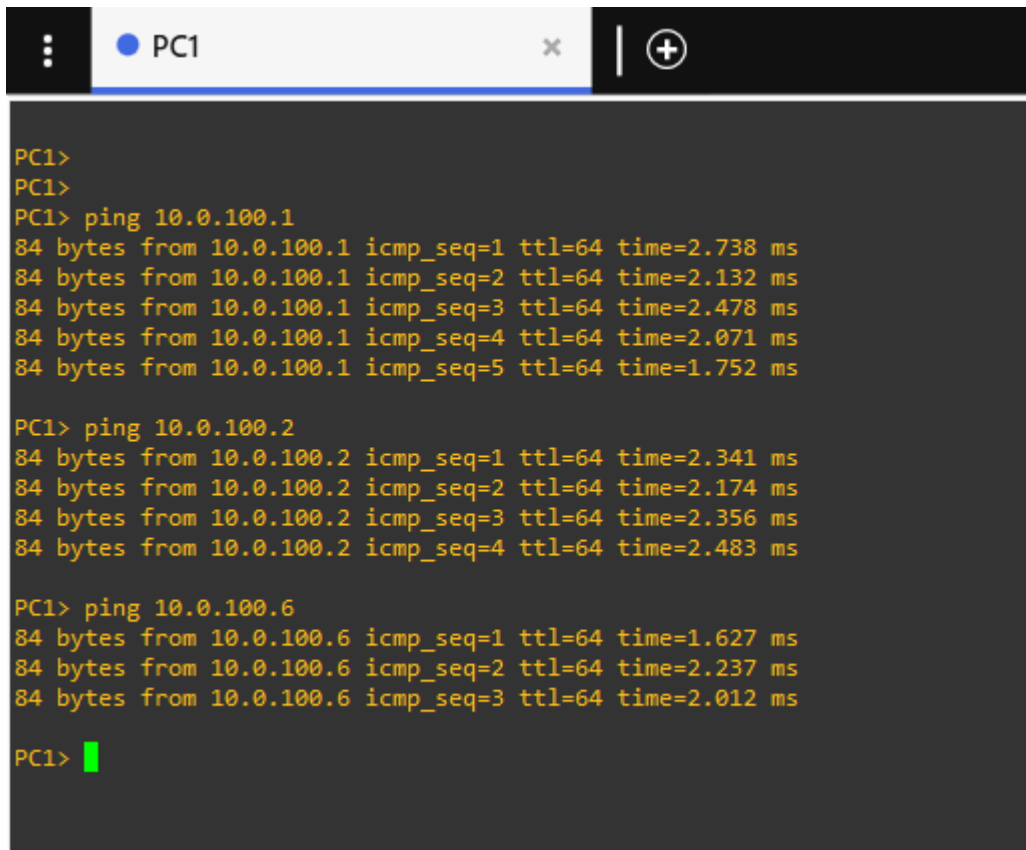
PC3> ip dhcp
DDORA IP 10.0.101.110/24 GW 10.0.101.254

PC3> █
```

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 6 Verificación LAN PC1



```
PC1>
PC1>
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=64 time=2.738 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=64 time=2.132 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=64 time=2.478 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=64 time=2.071 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=64 time=1.752 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=64 time=2.341 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=64 time=2.174 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=64 time=2.356 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=64 time=2.483 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.627 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=2.237 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=2.012 ms

PC1> █
```

PC2 debería hacer ping con éxito a:

- D1: 10.0.102.1
- D2: 10.0.102.2

Figura 7 PC2 ping D1: 10.0.102.1 D2: 10.0.102.2

```
1
PC2>
PC2>
PC2>
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=64 time=2.450 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=64 time=2.180 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=64 time=1.898 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=64 time=1.588 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=64 time=2.039 ms

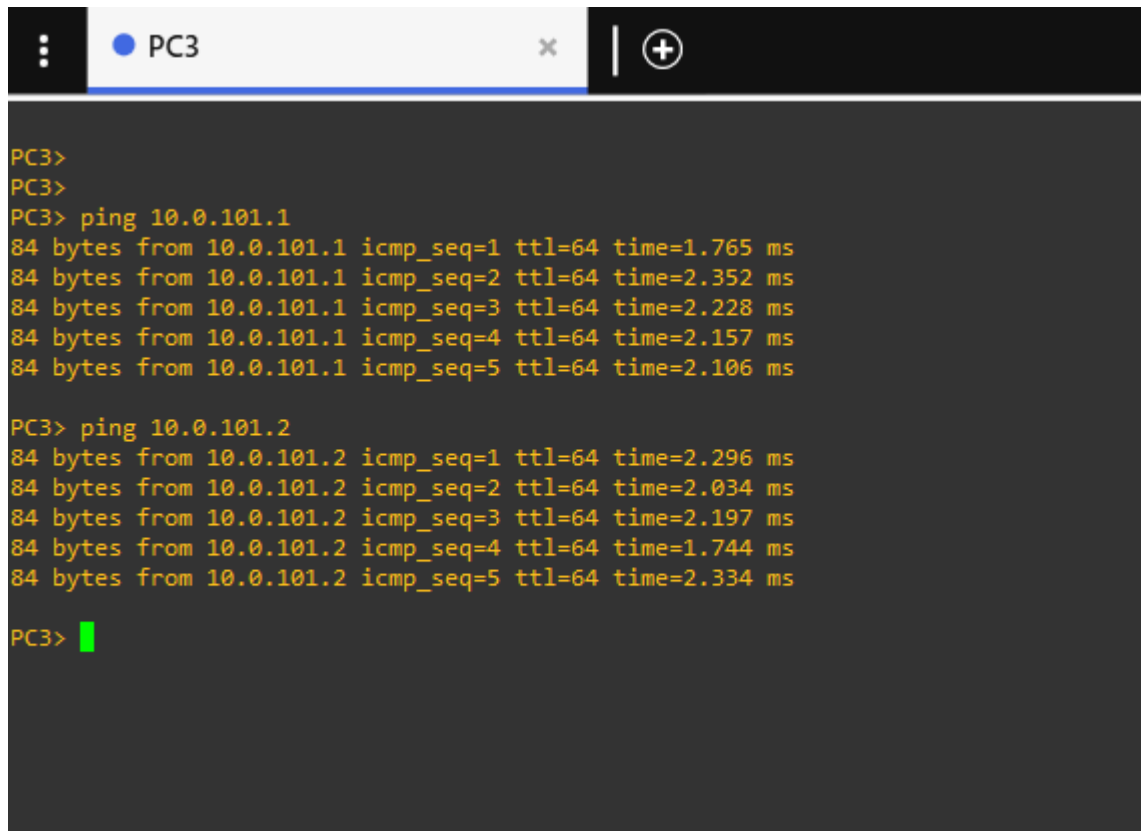
PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=64 time=2.453 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=64 time=2.135 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=64 time=1.921 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=64 time=2.096 ms

PC2> █
```

PC3 debería hacer ping con éxito a:

- D1: 10.0.101.1
- D2: 10.0.101.2

Figura 8 PC3 ping D1: 10.0.101.1 D2: 10.0.101.2



```
PC3>
PC3>
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=64 time=1.765 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=64 time=2.352 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=64 time=2.228 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=64 time=2.157 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=64 time=2.106 ms

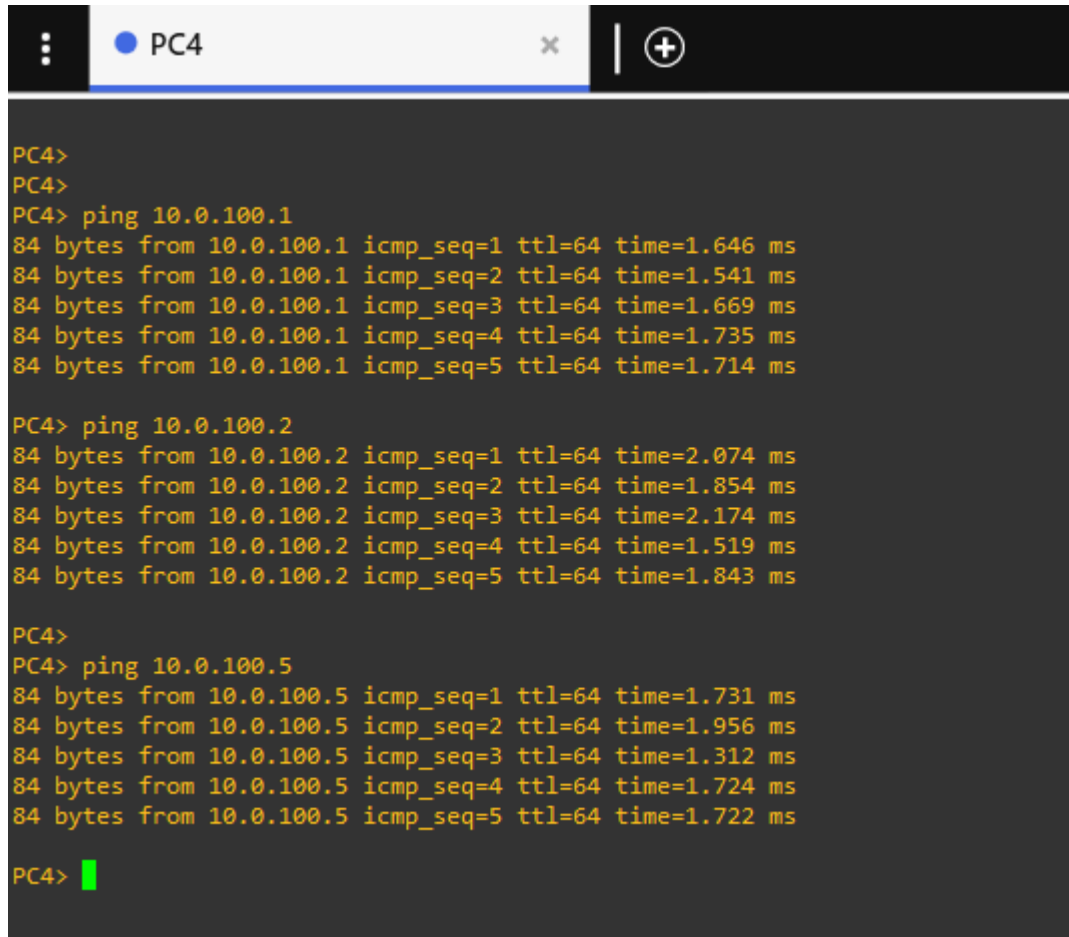
PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=64 time=2.296 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=64 time=2.034 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=64 time=2.197 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=64 time=1.744 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=64 time=2.334 ms

PC3> █
```

PC4 debería hacer ping con éxito a:

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

Figura 9 PC4 ping D1: 10.0.100.1 D2: 10.0.100.2: PC1: 10.0.100.5



```
PC4>
PC4>
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=64 time=1.646 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=64 time=1.541 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=64 time=1.669 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=64 time=1.735 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=64 time=1.714 ms

PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=64 time=2.074 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=64 time=1.854 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=64 time=2.174 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=64 time=1.519 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=64 time=1.843 ms

PC4>
PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=1.731 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=1.956 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.312 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.724 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.722 ms

PC4> █
```

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 Ethernet 0/0
```

```
D1(config-router)#passive-interface Ethernet 0/1
```

```
D1(config-router)#passive-interface Ethernet 0/2
```

```
D1(config-router)#passive-interface Ethernet 0/3
```

```
D1(config-router)#passive-interface Ethernet 1/0
```

```
D1(config-router)#passive-interface Ethernet 1/1
```

```
D1(config-router)#passive-interface Ethernet 1/2
```

```
D1(config-router)#passive-interface Ethernet 1/3
```

```
D1(config-router)#passive-interface Ethernet 2/0
```

```
D1(config-router)#passive-interface Ethernet 2/1
```

```
D1(config-router)#passive-interface Ethernet 2/2
```

```
D1(config-router)#passive-interface Ethernet 2/3
```

```
D1(config-router)#passive-interface Ethernet 3/0
```

```
D1(config-router)#passive-interface Ethernet 3/1
```

```
D1(config-router)#passive-interface Ethernet 3/2
```

```
D1(config-router)#passive-interface Ethernet 3/3
```

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

```
D2(config-router)#passive-interface Ethernet 0/0
```

```
D2(config-router)#passive-interface Ethernet 0/1
```

```
D2(config-router)#passive-interface Ethernet 0/2
```

```
D2(config-router)#passive-interface Ethernet 0/3
D2(config-router)#passive-interface Ethernet 1/0
D2(config-router)#passive-interface Ethernet 1/1
D2(config-router)#passive-interface Ethernet 1/2
D2(config-router)#passive-interface Ethernet 1/3
D2(config-router)#passive-interface Ethernet 2/0
D2(config-router)#passive-interface Ethernet 2/1
D2(config-router)#passive-interface Ethernet 2/2
D2(config-router)#passive-interface Ethernet 2/3
D2(config-router)#passive-interface Ethernet 3/0
D2(config-router)#passive-interface Ethernet 3/1
D2(config-router)#passive-interface Ethernet 3/2
D2(config-router)#passive-interface Ethernet 3/3
```

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 E1/0
 - R1(config-if)#ipv6 ospf 6 area 0
 - R1(config-if)#int E1/2
 - R1(config-if)#ipv6 ospf 6 area 0
- R3(config)#int E1/2
 - R3(config-if)#ipv6 ospf 6 area 0
 - R3(config-if)#int E1/1
 - R3(config-if)#ipv6 ospf 6 area 0
- D1(config)#int E0/0
 - 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 E0/0
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 Ethernet 0/0
D1(config-rtr)#passive-interface Ethernet 0/1
D1(config-rtr)#passive-interface Ethernet 0/2
D1(config-rtr)#passive-interface Ethernet 0/3
D1(config-rtr)#passive-interface Ethernet 1/0
D1(config-rtr)#passive-interface Ethernet 1/1
D1(config-rtr)#passive-interface Ethernet 1/2
D1(config-rtr)#passive-interface Ethernet 1/3
D1(config-rtr)#passive-interface Ethernet 2/0
D1(config-rtr)#passive-interface Ethernet 2/1
D1(config-rtr)#passive-interface Ethernet 2/2
```

```
D1(config-rtr)#passive-interface Ethernet 2/3
D1(config-rtr)#passive-interface Ethernet 3/0
D1(config-rtr)#passive-interface Ethernet 3/1
D1(config-rtr)#passive-interface Ethernet 3/2
D1(config-rtr)#passive-interface Ethernet 3/3
```

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

```
D2(config-rtr)#passive-interface Ethernet 0/0
D2(config-rtr)#passive-interface Ethernet 0/1
D2(config-rtr)#passive-interface Ethernet 0/2
D2(config-rtr)#passive-interface Ethernet 0/3
D2(config-rtr)#passive-interface Ethernet 1/0
D2(config-rtr)#passive-interface Ethernet 1/1
D2(config-rtr)#passive-interface Ethernet 1/2
D2(config-rtr)#passive-interface Ethernet 1/3
D2(config-rtr)#passive-interface Ethernet 2/0
D2(config-rtr)#passive-interface Ethernet 2/1
D2(config-rtr)#passive-interface Ethernet 2/2
D2(config-rtr)#passive-interface Ethernet 2/3
D2(config-rtr)#passive-interface Ethernet 3/0
D2(config-rtr)#passive-interface Ethernet 3/1
D2(config-rtr)#passive-interface Ethernet 3/2
D2(config-rtr)#passive-interface Ethernet 3/3
```

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

Figura 10 sesion radius R1.

```
R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: raduser
Password:

R1#
```

Figura 11 sesion radius R3

```
R3 con0 is now available

Press RETURN to get started.

User Access Verification
Username: raduser
Password:
R3#
```

Figura 12 sesion radius D1

```
D1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: raduser
Password:

D1#
```

Figura 13 sesion radius A1

```
A1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: raduser
Password:

A1#
```

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 CINDY CAROLINA
- 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

Se destaca los programas asimilados durante nuestro aprendizaje de habilidades prácticas como lo son el packet tracer y el GNS3 los cuales son una herramienta para entender mejor las redes y sus protocolos de enrutamiento como su profundización más precisa y comprensión del vital funcionamiento de las redes en nuestro día a día.

Con el desarrollo de las pruebas de habilidades prácticas de CCNP, es posible adquirir las capacidades necesarias para administrar equipos de red (como enrutadores y conmutadores), utilizar recursos y herramientas para establecer conexiones de red y resolver problemas que surjan.

Finalmente, el desarrollo de la prueba de habilidades prácticas permitió identificar que competencias y habilidades se obtuvieron a través del desarrollo del curso y que otras debieron ser reforzadas con el fin de lograr ofrecer una solución al problema planteado.

Es de gran satisfacción saber que el escenario planteado es totalmente orientado a problemas reales, esto nos hace estar preparados en gran medida para afrontar los retos profesionales que nos esperan.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

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. <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

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. <https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx>

UNAD (2015). Switch CISCO -Procedimientos de instalación y configuración del IOS [OVA]. <https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dq>