DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

PAOLA ANDREA CORREA SUAREZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

PAOLA ANDREA CORREA SUAREZ

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
TULUA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

TULUA, 29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física, son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.

IPv6: es la nueva versión del protocolo IP, ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual IPv4, en esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia se quitaron o se hicieron opcionales, agregándose nuevas características.

DNS: corresponde a las siglas en inglés de “Domain Name System”, es decir, “Sistema de nombres de dominio”, este sistema es básicamente la agenda telefónica de la Web que organiza e identifica dominios.

ENRUTAMIENTO: es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta, para encontrar esa ruta mas óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda, etc.

DHCP: es un servidor de Red el cual permite una asignación automática de direcciones IP, Gateway predeterminadas, así como otros parámetros de red que necesiten los clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problemas dentro de la red.

RESUMEN

Por medio del siguiente documento se desarrolla la actividad del escenario propuesto en el Diplomado de profundización CISCO, donde se pudo colocar a prueba los conocimientos adquiridos en el transcurso de la carrera de ingeniería en telecomunicaciones desde el curso de CCNP donde se tuvo la oportunidad de realizar la asignación IP a los equipos hosts y routers de la red, asignar dirección de Gateway para comunicarse con los demás hosts de dicha red, una vez configurado cada uno de los hosts se logró usar el protocolo de enrutamiento por medio de diversos comandos observados y tratados en el contenido del trabajo.

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

ABSTRACT

Through the following document, the activity of the scenario proposed in the CISCO in-depth Diploma is developed, where the knowledge acquired in the course of the telecommunications engineering career from the CCNP course was put to the test, where there was the opportunity to carry out assigning IP to the hosts and routers on the network, assigning the gateway address to communicate with the other hosts on that network, once each of the hosts was configured, the routing protocol was used through various commands observed and treated in the content of the work.

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

INTRODUCCIÓN

En el siguiente documento se realizarán actividades de profundización de CISCO CCNP, en donde se evidenciarán actividades de configuración bajo prácticas de switching mediante configuraciones que van desde protocolos como STP, segmentación de redes con VLANs a nivel corporativo, pudiendo evitar factores que afectan el buen funcionamiento de una RED corporativa como son las colisiones de broadscast bajo múltiples escenarios presentes una red jerárquica que converge entre sí.

De igual forma se abordará bajo configuración IOS en los routers protocolos de enrutamiento dinámico, lo que facilita la interconexión de redes de diferente segmento, típicamente se usan en conexión de tipo WAN, pero igual forma puede ser utilizado a nivel LAN, en dependencia de las necesidades de requerimientos de infraestructura de redes de comunicación que se trabaje.

La actividad se desarrolla por medio de la aplicación de Cisco Packet Tracer donde se realiza uno a uno de los puntos indicados en la guía, con el fin de cumplir con los requisitos propuestos en el Diplomado de profundización de CISCO de manera correcta y confiada de los conocimientos obtenidos en el transcurso del curso.

DESARROLLO

ESCENARIO 1

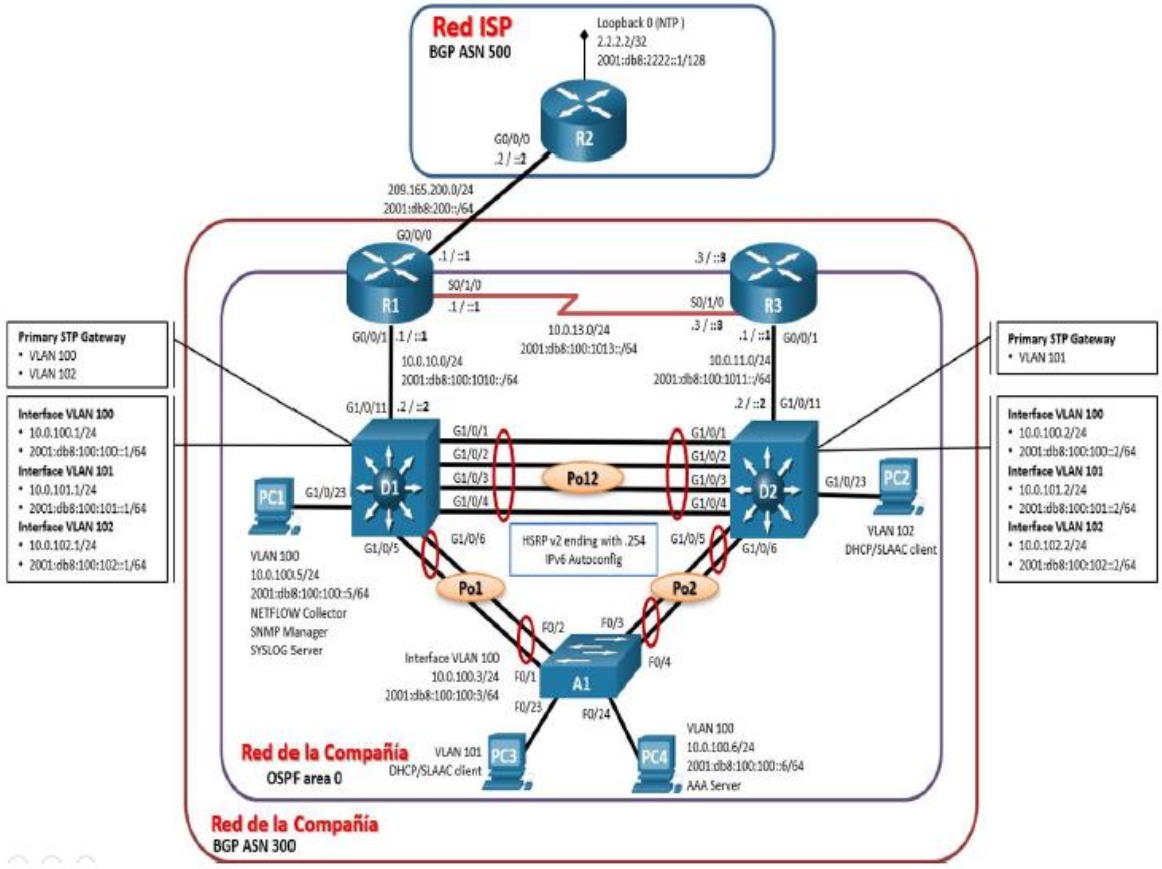

Figura 1 - Escenario 1

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

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

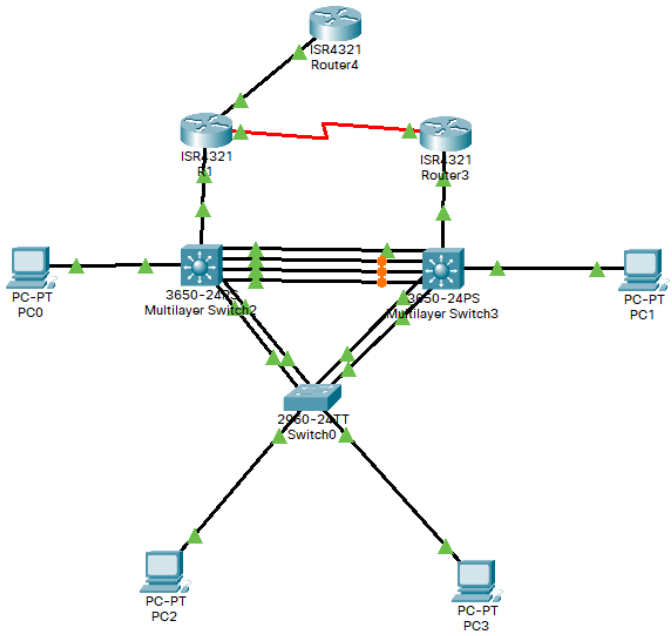

Figura 2 - Simulación de escenario 1

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:

   En este punto se realiza la configuración de los dispositivos con base a la tabla de direccionamiento de los Routers, Switches y los PC.

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

Tabla 1 – Tabla de direccionamiento

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
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
interface range g1/0/12-24
shutdown
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
interface range g1/0/12-24
shutdown
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

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

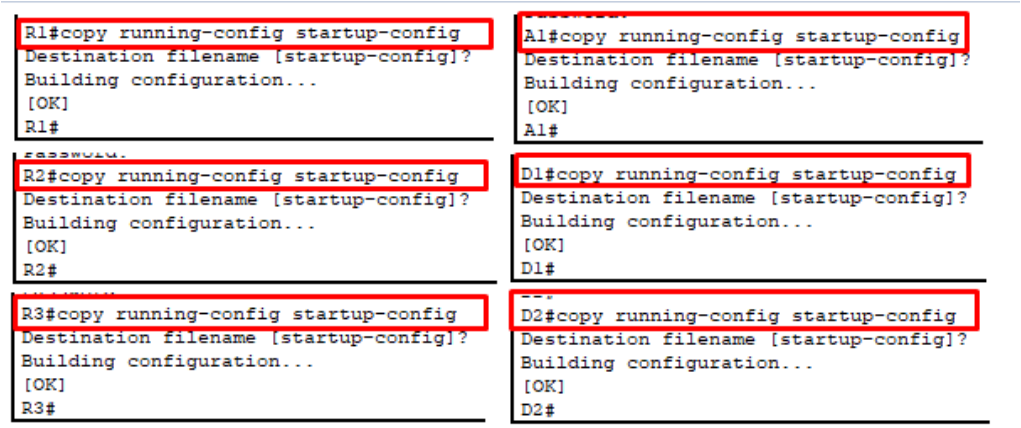

Figura 3 - Configuración running-config

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.

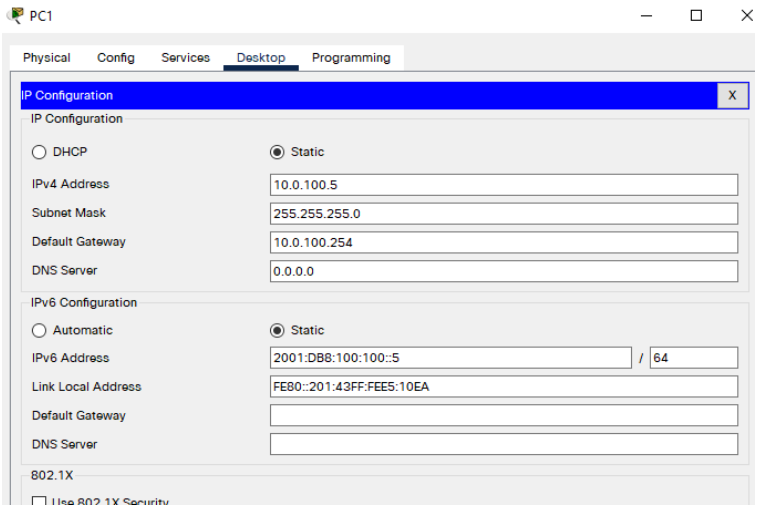

Figura 4 - Configuración host PC1

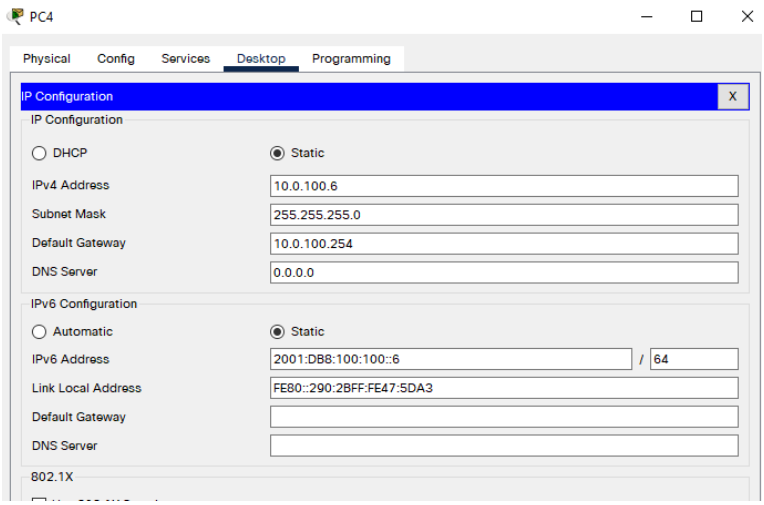

Figura 5 - Configuración host PC4

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. Habilite enlaces trunk 802.1Q entre:

- D1 and D2
- D1 and A1
- D2 and A1

2.2. En todos los switches cambie la VLAN nativa en los enlaces troncales. Use VLAN 999 como la VLAN nativa

D1 y D2

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
exit
interface GigabitEthernet1/0/2
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
exit
interface GigabitEthernet1/0/3
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
exit
interface GigabitEthernet1/0/4
switchport trunk native vlan 999
```

switchport trunk encapsulation dot1q
exit
interface GigabitEthernet1/0/5
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
exit
interface GigabitEthernet1/0/6
switchport trunk native vlan 999
switchport trunk encapsulation dot1q
exit

A1
interface fastEthernet 0/1
switchport trunk native vlan 999
switchport mode trunk
exit
interface fastEthernet 0/2
switchport trunk native vlan 999
switchport mode trunk
exit
interface fastEthernet 0/3
switchport trunk native vlan 999
switchport mode trunk
exit
interface fastEthernet 0/4
switchport trunk native vlan 999
switchport mode trunk
exit

2.3. En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP). Use Rapid Spanning Tree (RSPT)

D1, D2 y A1
Se utiliza la misma configuración para cada switch
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). Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

D1
Spanning-tree vlan 100-102,999 priority 24576

D2
Spanning-tree vlan 100-102,999 priority 28672

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 a A1 – Port channel 1
• D2 a A1 – Port channel 2

D1
interface range g1/0/1-4
channel-group 12 mode active
channel-protocol lacp
exit
interface port-channel 12
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface range g1/0/5-6
channel-group 1 mode active
channel-protocol lacp
exit
interface port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
exit

D2
interface range g1/0/1-4
channel-group 12 mode active
channel-protocol lacp
exit
interface port-channel 12
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface range g1/0/5-6
channel-group 2 mode active
channel-protocol lacp
exit
interface port-channel 2
switchport trunk encapsulation dot1q
switchport mode trunk
exit

A1
interface range f0/1-2
channel-group 1 mode active

channel-protocol lacp
exit
interface port-channel 1
switchport mode trunk
exit
interface range f0/3-4
channel-group 2 mode active
channel-protocol lacp
exit
interface port-channel 2
switchport mode trunk
exit

2.6. En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4. Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

D1
interface GigabitEthernet1/0/23
switchport access vlan 100
switchport mode access
switchport nonegotiate

D2
interface GigabitEthernet1/0/23
switchport access vlan 102
switchport mode access
switchport nonegotiate

A1
interface FastEthernet0/23
switchport access vlan 101
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 100
switchport mode access

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

ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0

default-router 10.0.101.254
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
ip dhcp pool pc2
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
dns-server 10.0.102.254

2.8. 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

PC2 debería hacer ping con éxito a:
• D1: 10.0.102.1
• D2: 10.0.102.2

PC3 debería hacer ping con éxito a:
• D1: 10.0.101.1
• D2: 10.0.101.2

PC4 debería hacer ping con éxito a:
• D1: 10.0.100.1
• D2: 10.0.100.2
• PC1: 10.0.100.5

Los ping que se hicieron desde PC1, PC, PC3 y PC4 fueron exitosos

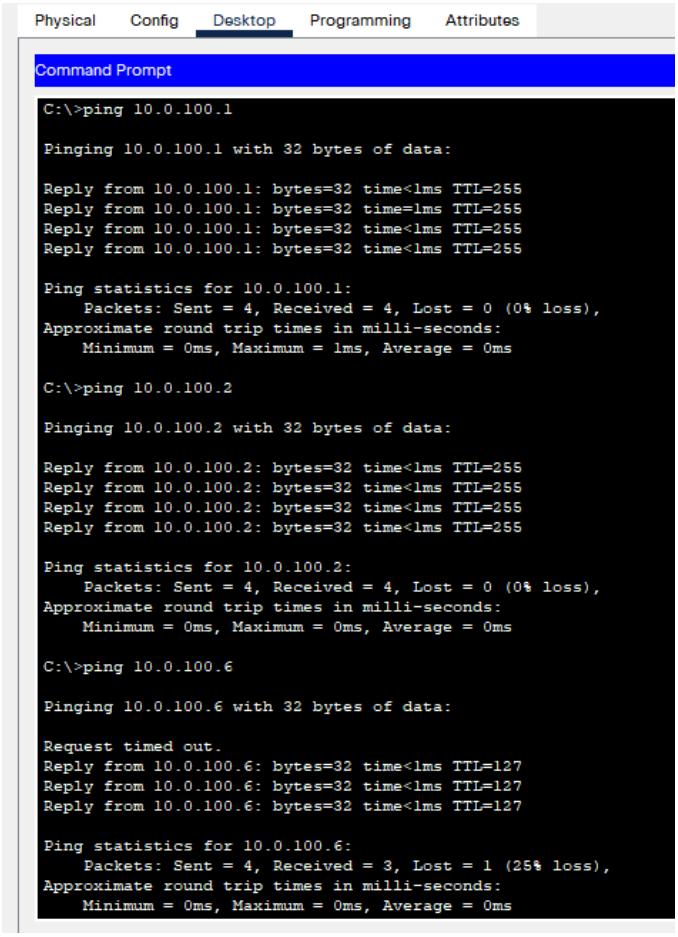

Figura 6 - Ping de D1, D2 y PC4 desde PC1

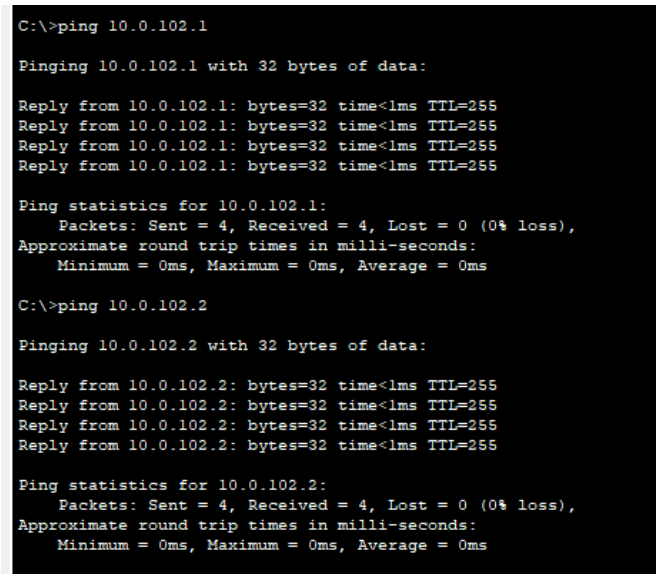

Figura 7 – Ping de D1 y D2 desde PC2

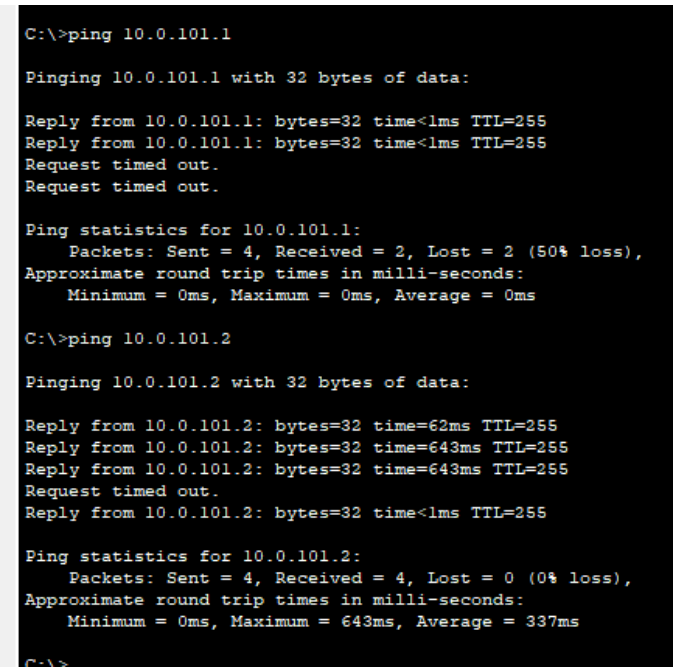

Figura 8 - Ping de D1 y D2 desde PC3

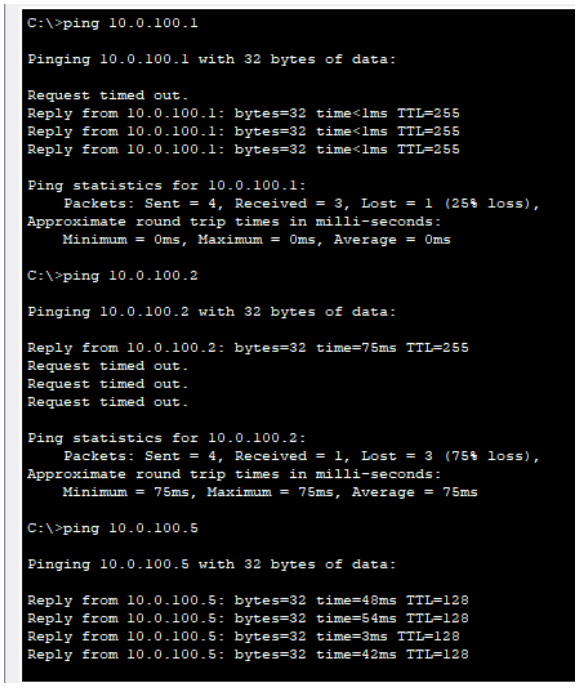

Figura 9 - Ping D1, D2 y PC1 desde PC4

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.

3.1. En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0. Use OSPF Process ID 4 y asigne los siguientes router-IDs:

• R1: 0.0.4.1
• R3: 0.0.4.3
• D1: 0.0.4.131
• D2: 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.
• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv2 en:

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

R1

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

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
```

D1

```
router ospf 4
router-id 0.0.4.131
log-adjacency-changes
passive-interface default
```

no passive-interface GigabitEthernet1/0/11
network 10.0.10.0 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

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 Compañia" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0. Use OSPF Process ID 6 y asigne los siguientes router-IDs:
• R1: 0.0.6.1
• R3: 0.0.6.3
• D1: 0.0.6.131
• D2: 0.0.6.132

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.
• En R1, no publique la red R1 – R2.
• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv3 en:
• D1: todas las interfaces excepto G1/0/11
• D2: todas las interfaces excepto G1/0/11

R1
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
log-adjacency-changes

R3
ipv6 router ospf 6
router-id 0.0.6.3
log-adjacency-changes

D1
ipv6 router ospf 6
router-id 0.0.6.131
log-adjacency-changes
passive-interface GigabitEthernet1/0/11

D2
ipv6 router ospf 6
router-id 0.0.6.132
log-adjacency-changes

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.
• Una ruta estática predeterminada IPv6.

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

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).

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. Configure dos rutas resumen estáticas a la interfaz Null 0:
• Una ruta resumen IPv4 para 10.0.0.0/8.
• Una ruta resumen IPv6 para 2001:db8:100::/48.

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

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.
• Anuncie la red 10.0.0.0/8.

En IPv6 address family:
• Deshabilite la relación de vecino IPv4.
• Habilite la relación de vecino IPv6.
• Anuncie la red 2001:db8:100::/48.

R2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
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
network 0.0.0.0
redistribute static
#en packet tracert no hay address-family

R1
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
#en packet tracert no hay address-family

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 host en la “Red de la Compañía”.

4.1. En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1. Cree dos IP SLAs.
• Use la SLA número 4 para IPv4.
• Use la SLA número 6 para IPv6.

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

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

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.
• Use el número de rastreo 4 para la IP SLA 4.
• Use el número de rastreo 6 para la IP SLA 6.

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

4.2. En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1. Cree IP SLAs.
• Use la SLA número 4 para IPv4.
• Use la SLA número 6 para IPv6.

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

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

Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.
• Use el número de rastreo 4 para la IP SLA 4.
• Use el número de rastreo 6 para la SLA 6.

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

#No se pudo realizar el punto debido que en packet tracer no hay ip SLA

4.3. En D1 configure HSRPv2. D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:
• Asigne la dirección IP virtual 10.0.100.254.
• Establezca la prioridad del grupo en 150.
• Habilite la preferencia (preemption).
• Rastree el objeto 4 y decremente en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:
• Asigne la dirección IP virtual 10.0.101.254.
• Habilite la preferencia (preemption).
• Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:
• Asigne la dirección IP virtual 10.0.102.254.
• Establezca la prioridad del grupo en 150.
• Habilite la preferencia (preemption).
• Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:
• Asigne la dirección IP virtual usando ipv6 autoconfig.
• Establezca la prioridad del grupo en 150.
• Habilite la preferencia (preemption).
• Rastree el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:
• Asigne la dirección IP virtual usando ipv6 autoconfig.
• Habilite la preferencia (preemption).
• Registre el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:
• Asigne la dirección IP virtual usando ipv6 autoconfig.
• Establezca la prioridad del grupo en 150.
• Habilite la preferencia (preemption).
• Rastree el objeto 6 y decremente en 60.

D1

```
interface Vlan100
mac-address 000c.8558.5301
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
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 000c.8558.5302
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
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 116 ipv6 autoconfig
standby 116 preempt
!
interface Vlan102
mac-address 000c.8558.5303
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
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
```

D2

```
interface Vlan100
mac-address 00e0.f99c.7701
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
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 106 ipv6 autoconfig
standby 106 preempt
!
interface Vlan101
mac-address 00e0.f99c.7702
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
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 00e0.f99c.7703
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
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. En esta configuración se maneja todos los mecanismos de seguridad en todos los dispositivos.

5.1. En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT. Contraseña: cisco12345cisco

R1, R2, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos

service password-encryption
enable password Level 15 cisco12345cisco

5.2. En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT. Detalles de la cuenta encriptada SCRYPT:
• Nombre de usuario Local: sadmin
• Nivel de privilegio 15
• Contraseña: cisco12345cisco

R1, R2, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos

username sadmin privilege 15 secret cisco12345cisco

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

R1, R2, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos

aaa new-model

5.4. En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS. Especificaciones del servidor RADIUS.:
• Dirección IP del servidor RADIUS es 10.0.100.6.
• Puertos UDP del servidor RADIUS son 1812 y 1813.
• Contraseña: $trongPass

R1, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos excepto para R2

radius-server host 10.0.100.6 auth-port 1812 key $trongPass

5.5. En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA. Especificaciones de autenticación AAA:
• Use la lista de métodos por defecto
• Valide contra el grupo de servidores RADIUS
• De lo contrario, utilice la base de datos local.

R1, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos excepto para R2

aaa authentication login default group radius local
line vty 0 15

login authentication default
exit

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.

la autenticación del usuario raduser funciona

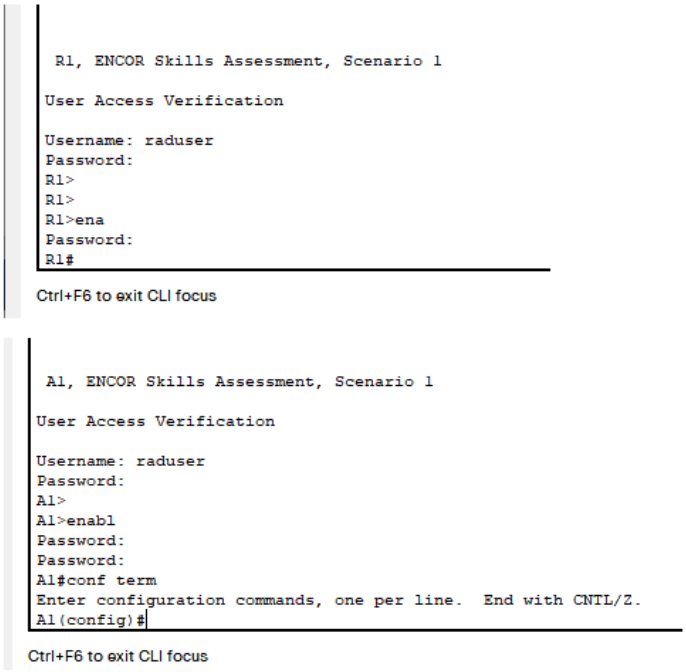

Figura 10 - Se valida su funcionamiento en R1 y A1

Parte 6. Configure las funciones de Administración de Red
En esta parte, debe configurar varias funciones de administración de red.

En esta sección se realizó la parte de configuración del reloj local actual, el NTP maestro en R2.

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

R1, R2, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos

clock timezone UTC -5

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

R2
ntp master 3

6.3. Configure NTP en R1, R3, D1, D2, y A1. Configure NTP de la siguiente manera:
• R1 debe sincronizar con R2.
• R3, D1 y A1 para sincronizar la hora con R1.
• D2 para sincronizar la hora con R3.

R1
ntp server 209.165.200.226

R3, D1, A1
ntp server 10.0.10.1

D2
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.

6.5. Configure SNMPv2c en todos los dispositivos excepto R2. Especificaciones de SNMPv2:

• Unicamente se usará SNMP en modo lectura (Read-Only).
• Limite el acceso SNMP a la dirección IP de la PC1.
• Configure el valor de contacto SNMP con su nombre.
• Establezca el community string en ENCORSA.
• 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

R1, R3, A1, D1 y D2
Se utiliza la misma configuración para cada uno de los dispositivos excepto para R2

logging host 10.0.100.5
logging trap
logging on
snmp-server community ENCORSA ro

CONCLUSIONES

Con el presente trabajo se pudo obtener mayores conocimientos en la parte práctica para el proceso de crear y configurar todo tipo de topología a la que nos toque enfrentarnos en el transcurso del ámbito profesional.

La función principal de la actividad presentada en el diplomado de profundización CISCO es ayudar a fortalecer los conocimientos que se adquirieron en el transcurso de la carrera profesional, y apoyar en la investigación para que el estudiante tenga las bases necesarias para enfrentar cualquier tipo de escenario que se presente a lo largo del camino laboral.

En el transcurso del desarrollo de la actividad se logró cumplir con cada uno de los puntos planteados en la guía, se pudo hacer de manera satisfactoria el montaje de la topología en Packet Tracer, donde se realizó la configuración de la red, los ping realizados dieron respuestas satisfactorias y los protocolos que se configuraron quedaron de manera operativa.

Se pudo profundizar en el estudio de CISCO CCNP bajo los temas de switching STP, y enrutamiento dinámico que se utiliza para lograr una computación a nivel WAN y LAN.

BIBLIOGRÁFIA

Ariganello E, Técnicas de Configuración de Routers CISCO. Recuperado de https://books.google.com.co/books?id=Oo-fDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Comandos básicos de un routers Cisco. Recuperado el 18 de octubre de 2013 https://alexalvarez0310.wordpress.com/category/comandos-basicos-de-un-router-cisco/

Hernández E., Imágenes Cisco en GNS3 para CCNP Enterprise. Recuperado de https://www.youtube.com/watch?v=GzxDzYn7ZBI&ab_channel=EdsonHernandez