DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP.

VICTOR CLEMENTE ROSERO PERAFAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
LA HORMIGA
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP.

VICTOR CLEMENTE ROSERO PERAFAN

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
LA HORMIGA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

HORMIGA, 5 de diciembre 2021

AGRADECIMIENTOS

Primero dar gracias a nuestro creador por permitirnos estar con vida, y poder realizar el presente trabajo por otra parte a la universidad nacional abierta y a distancia UNAD por permitirnos ser miembros de tan prestigiosa universidad, a los compañeros les doy las gracias por los aportes en el foro por último a los señores tutores por brindarnos sus conocimientos el tiempo y paciencia con nosotros los estudiantes.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

IP estática: la dirección IP estática se configura manualmente en el dispositivo de red, como enrutadores y conmutadores, y también en servidores.

IP dinámica: es la que se puede asignar automáticamente a un dispositivo a través del Protocolo de configuración dinámica de host (DHCP). Es mejor utilizar direcciones IP dinámicas en dispositivos finales, como PC.

El protocolo de árbol de expansión (STP):es un protocolo de red diseñado para evitar bucles de capa 2. Está estandarizado como protocolo IEEE 802.D. STP bloquea algunos puertos en conmutadores con enlaces redundantes para evitar tormentas de difusión y garantizar una topología sin bucles. Con STP en su lugar, puede tener enlaces redundantes entre conmutadores para proporcionar redundancia.

IPv6: es la versión más reciente del protocolo IP. IPv6 se desarrolló para superar muchas deficiencias de IPv4, entre las que destaca el problema del agotamiento de la dirección IPv4. A diferencia de IPv4, que solo tiene alrededor de 4,3 mil millones (2 elevados a 32) direcciones disponibles, IPv6 permite 3,4 × 10 elevado a 38 direcciones.

IEEE 802.1Q: es uno de los protocolos de etiquetado de VLAN compatibles con los conmutadores de Cisco. Este estándar fue creado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), por lo que es un estándar abierto y se puede utilizar en conmutadores que no sean de Cisco.

RESUMEN

Este informe es una demostración de que como profesional en electrónica soy capaz de resolver muchas temáticas relacionadas con las redes de comunicación, como lo evidencio en el presente informe donde detallo que comandos corresponden para cada tipo de configuración. Todo este saber lo he demostrado en las actividades de CISCO como de CCNP y en este momento lo aplico como opción de grado.

Aplicando mis habilidades desarrolle de manera completa este informe al establecer una accesibilidad de un dispositivo a otro, a través de muchas configuraciones necesarias que permitieron identificar varios datos como lo son; el nombre, las direcciones, las interfaces, la seguridad, los protocolos de enrutamiento y la hora entre otras configuraciones que sirven para establecer una conexión en la red.

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

ABSTRACT

This report is a demonstration that as electronics professional I am capable of solving many issues related to communication networks, as evidenced in this report where I detail which commands correspond to each type of configuration. All this knowledge I have shown in the activities of CISCO and CCNP and at this moment I apply it as a degree option.

Applying my skills, I fully developed this report by establishing accessibility from one device to another, through many necessary configurations that allowed identifying various data as they are; the name, addresses, interfaces, security, routing protocols and time, among other settings used to establish a connection on the network.

Keywords: CISCO, CCNP, Routing, Networks, Electronics.

INTRODUCCIÓN

Este trabajo se realizó con el fin de demostrar los conocimientos aprendidos en el área de las redes de comunicación más exactamente en establecer una conectividad de manera satisfactoria.

Para esto se resolvió un escenario en gns3 cuya topología se diseñó con tres routers, tres switchs y 4 computadores. Para posteriormente pasar a configurar cada dispositivo de acuerdo la interfaz, claro que como se realizó en gns3 el diseñó cambio en el número, como en el tipo de puerto, lo cual fue muy necesario tener presente para saber identificar cada dirección a que interface y dispositivo pertenece entre otros datos que permitieron que se desarrolle el paso a paso de esta actividad de manera completa.

Este desarrollo consta de seis partes dos de los cuales ya expliqué en el anterior párrafo para la tercera parte configuré con protocolos de enrutamiento como single-área OSPFv2 y OSPFv3 con área 0 en R1, R3, D1, y D2, otros protocolos empleados fueron: MP-BGP en R2 y MP-BGP en R1. En la parte cuatro se configuro HSRPv2 y se creó IP SLAS en D1 y D2. En la parte cinco y seis se protegió cada dispositivo con usuario contraseña también se colocó mi nombre como contacto, seguido de la configuración de la fecha y hora actual.

DESARROLLO

ESCENARIO PROPUESTO

Figura 1. Topología de red.

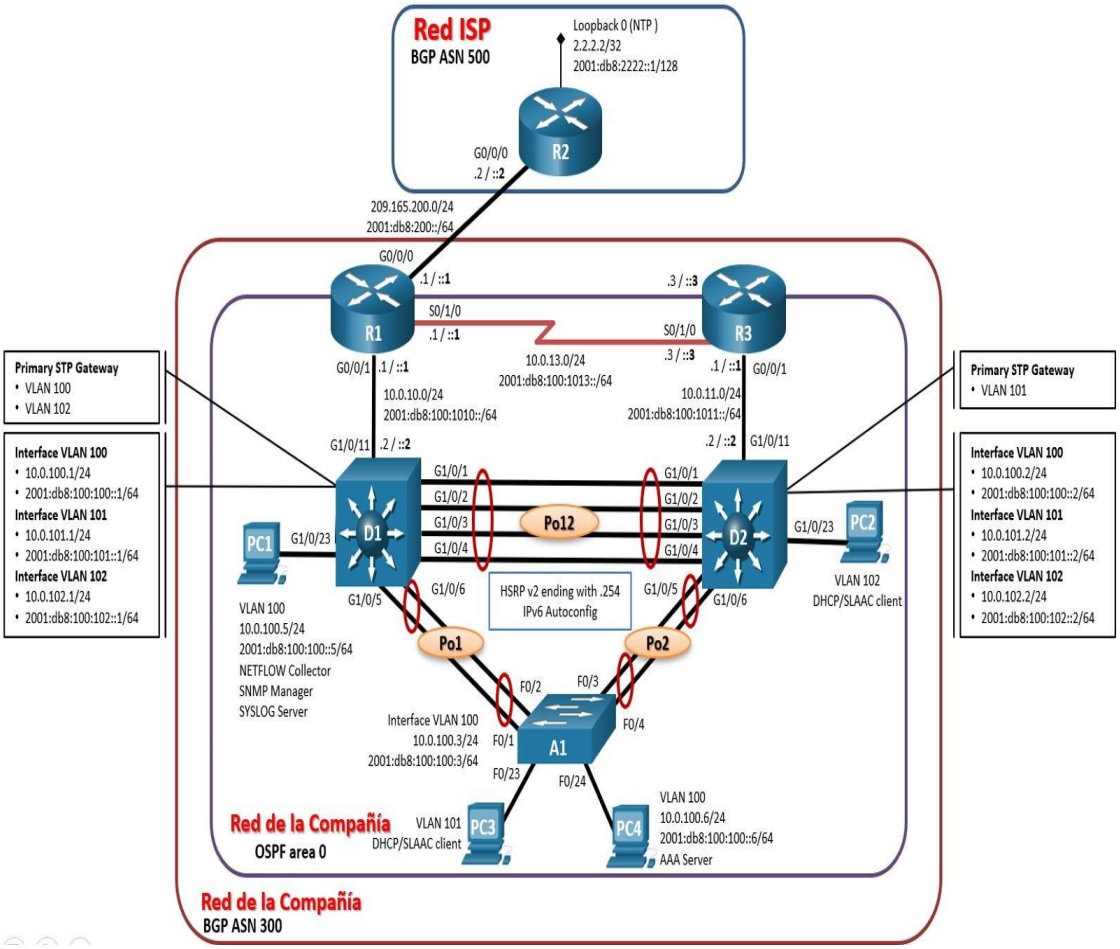


Tabla 1. Tabla de direccionamiento.

#	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

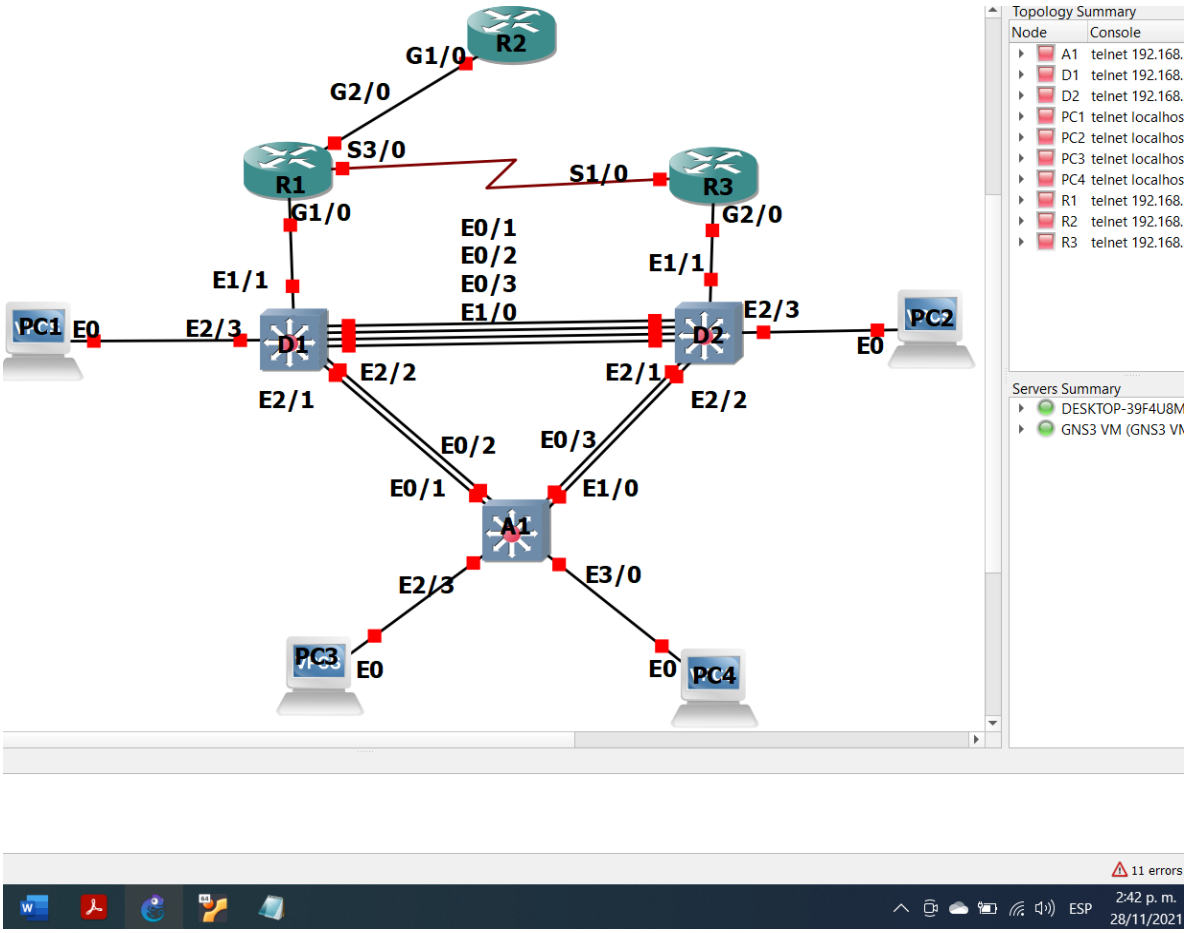
Parte 1.

Construir la red y configurar los parámetros básicos.

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. Diseño de topología realizada en GNS3.



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.

Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3 y switchs: según la tabla de direccionamiento configure las interfaces que corresponden a cada dispositivo.

Se procede a configurar cada uno de los enrutadores y Switch:

Desarrollo del ítem a.

ROUTER R1

```
R1#enable
R1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)# banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface g2/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface g1/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#ex
*Oct 18 02:38:33.263: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Oct 18 02:38:34.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
R1(config-if)#exit
R1(config)#interface s3/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

ROUTER 2

```
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g1/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
*Oct 18 03:05:57.211: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed
state to up
*Oct 18 03:05:58.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0, changed state to up
R2(config-if)#interface loopback 0
R2(config-if)#
*Oct 18 03:06:50.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback0, changed state to up
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

ROUTER 3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface g2/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
*Oct 18 03:30:39.899: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed
state to up
*Oct 18 03:30:40.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet2/0, changed state to up
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
*Oct 18 03:33:22.167: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R3(config-if)#exit
R3(config)#
*Oct 18 03:33:23.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial1/0, changed state to up
R3(config)#
```

Switch D1

```
D1#
D1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface e1/1
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
```

```
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range e0/0-3,e1/0,e1/2-3,e2/0-3,e3/0-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
```

Switch D2

```
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface e1/1
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

```
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range e0/0-3,e1/0,e1/2-3,e2/0-3,e3/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
```

Switch A1

```
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#hostname A1
A1(config)#ip routing
A1(config)#ipv6 unicast-routing
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
A1(config)#interface vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range e1/1-3,e2/0-3,e3/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
```

Desarrollo del ítem b.

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

Con el comando copy running-config startup guardo la configuración que realizado en cada Router y Switch.

Comando que se colocó en cada dispositivo.

R1(config)# copy running-config startup

R2(config)# copy running-config startup

R3(config)# copy running-config startup

D1#copy running-config startup

D2#copy running-config startup

Desarrollo del ítem c.

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.

Tabla 2. Realizo la configuración de las PC1 y PC4.

Dispositivo.	**Interfaz.**	**Dirección IPv4.**	**Dirección IPv6.**	**IPv6 Link-Local**
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC1	PC1> ip 10.0.100.5/24 Checking for duplicate address... PC1 : 10.0.100.5 255.255.255.0		De esta manera agregue la dirección IP a PC1.	Con el comando: **ip 10.0.100.5/24**
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64
PC4	PC4> ip 10.0.100.6/24 Checking for duplicate address... PC1 : 10.0.100.6 255.255.255.0		De esta manera agregue la dirección IP a PC4.	Con el comando: **ip 10.0.100.6/24**
PC3	PC3> ip dhcp		De esta manera agregue la dirección IP DHCP.	**ip dhcp**
PC2	PC2> ip dhcp		De esta manera agregue la dirección IP DHCP	**ip dhcp**

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 switchs debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Desarrollo de la parte 2.

Tabla 3. Códigos que emplee para cada tarea.

Tarea.	Comandos.	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches. interface range e0/1-3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk interface range e2/1-2 switchport trunk encapsulation dot1q switchport mode trunk interface range e0/1-3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk	Habilite enlaces trunk 802.1Q entre: En switch D1

	interface range e2/1-2 switchport trunk encapsulation dot1q switchport mode trunk spanning-tree mode rapid-pvst interface range e0/1-2 switchport trunk encapsulation dot1q switchport mode trunk interface range e0/3, e1/0 switchport trunk encapsulation dot1q switchport mode trunk	En switch D2 En switch A1.
2.2	En todos los switches cambie la VLAN nativaen los enlaces troncales. switchport trunk native vlan 999	Use VLAN 999 como la VLAN nativa. En switch D1, D2 y D3.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP) spanning-tree mode rapid-pvst spanning-tree portfast spanning-tree portfast	Use Rapid Spanning Tree (RSPT). En switch D1 y D2 se emplean los dos comandos. Solo en A1 se empleó este comando.

Tabla 4. Continuación de la parte 2.

Tarea.	Comandos.	Especificación
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). spanning-tree vlan 100,102 root primary spanning-tree vlan 101 root secondary spanning-tree vlan 101 root primary spanning-tree vlan 100,102 root secondary	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch. En Switch D1 configure como raíz primario y secundario. En Switch D2 configure como raíz primario y secundario.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de	Use los siguientes números de canales: • D1 a D2 – Port channel 12

	topología. channel-group 12 mode active channel-group 1 mode active channel-group 12 mode active channel-group 2 mode active channel-group 1 mode active channel-group 2 mode active	• D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2 En Switch D1 En Switch D2. En Switch A1.
2.6	En todos los switches, configure los puertos de acceso del host que seconectan a PC1, PC2, PC3 y PC4. interface e2/3 switchport mode Access switchport access vlan 100 spanning-tree portfast no shutdown exit	Configure los puertos de acceso con la configuración de VLAN adecuada, comose muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío. En Switch D1 con interface e2/3 hacia PC1.

	interface e2/3 switchport mode Access switchport access vlan 102 spanning-tree portfast no shutdown exit	En Switch D2 con interface e2/3 hacia PC2.
	interface e2/3 switchport mode access switchport access vlan 101 spanning-tree portfast no shutdown exit interface e3/0 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end	En Switch A1 con interfaces de conexión hacia PC3 y PC4. Con interface e2/3 conexión a PC3. Con interface e2/3 conexión a PC4.
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

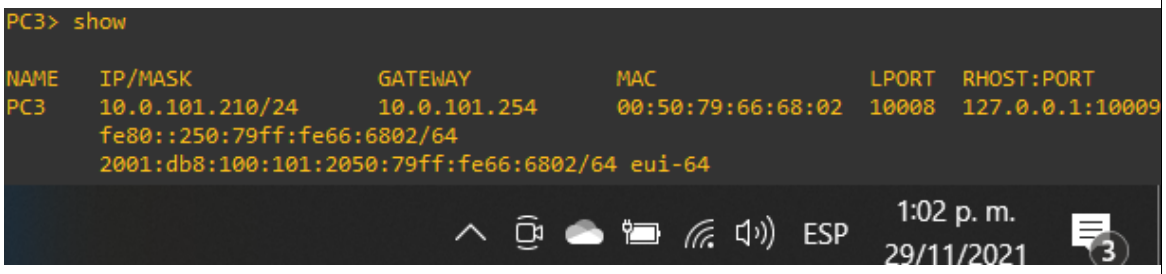
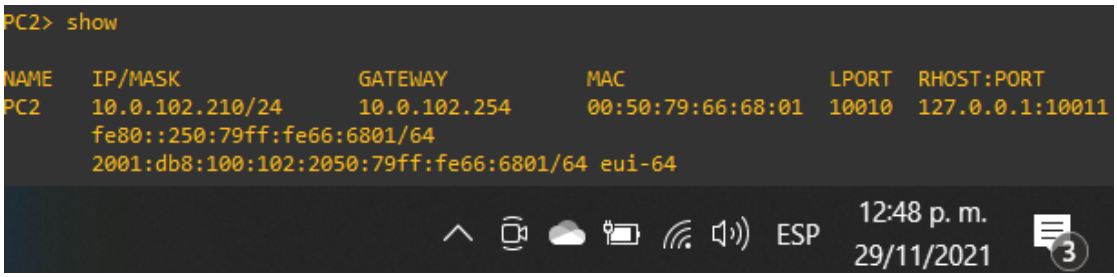
	PC3> ip dhcp DDORA IP 10.0.101.210/24 GW 10.0.101.254	PC3 lo configure como DHCP y por eso recibe direcciones IPv4 válidas y esto lo verifique en el PC3 con el comando show.
Figura 3. Verificación en PC3 de DHCP.  		
	PC2> ip dhcp DDORA IP 10.0.102.210/24 GW 10.0.102.254.	PC2 lo configure como DHCP y por eso recibe direcciones IPv4 válidas y esto lo verifique en el PC2 con el comando show.

Figura 4. Verificación en PC2 de DHCP.



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

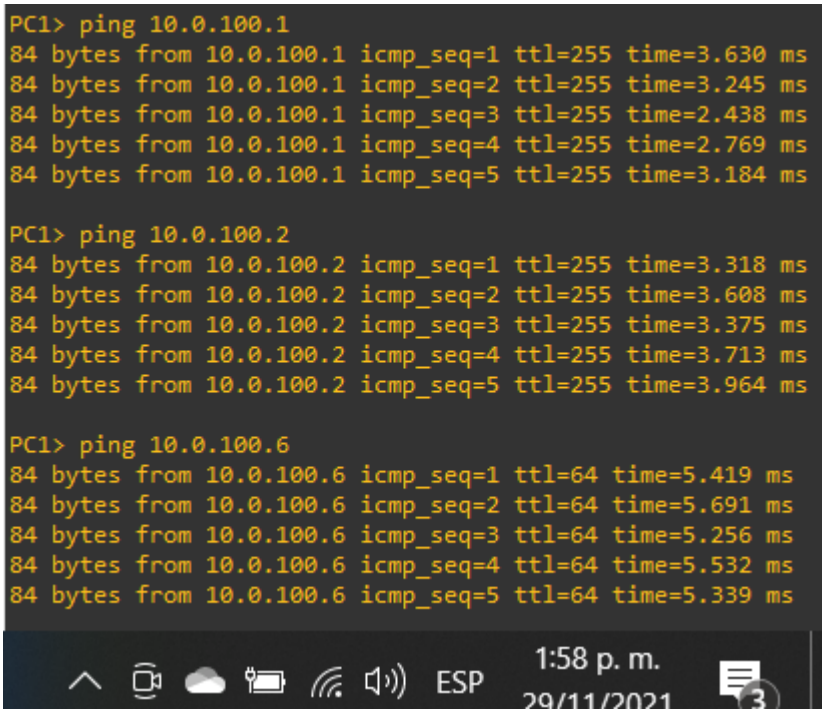
	Figura 5. Verificación de la conectividad en la LAN local en PC1. 	
	Verifique la conectividad de la LAN local.	PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2

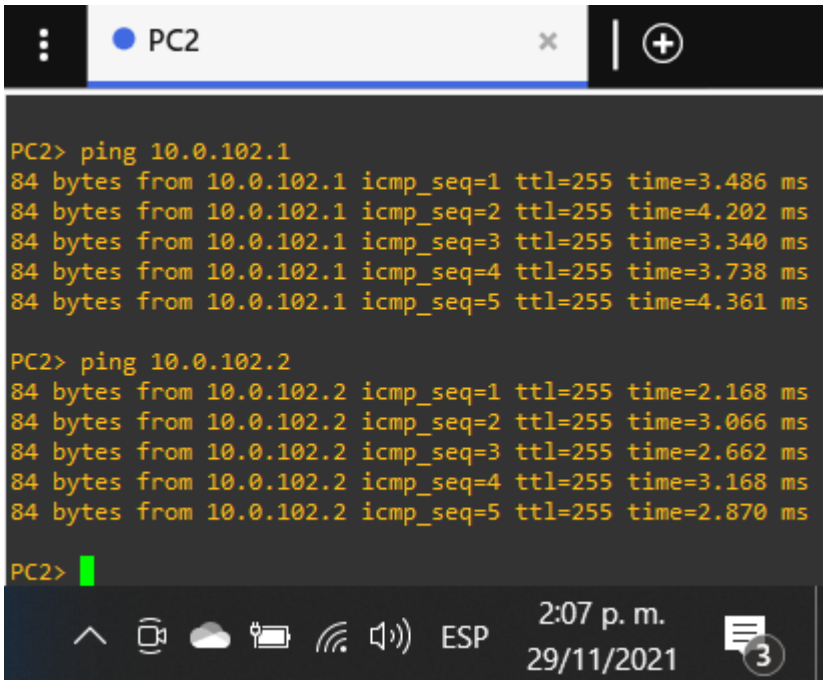
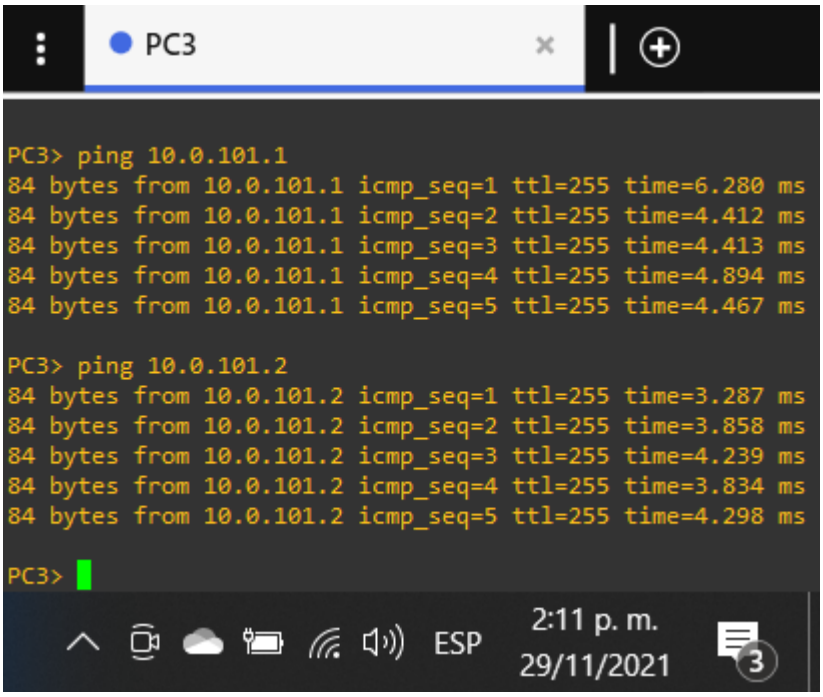
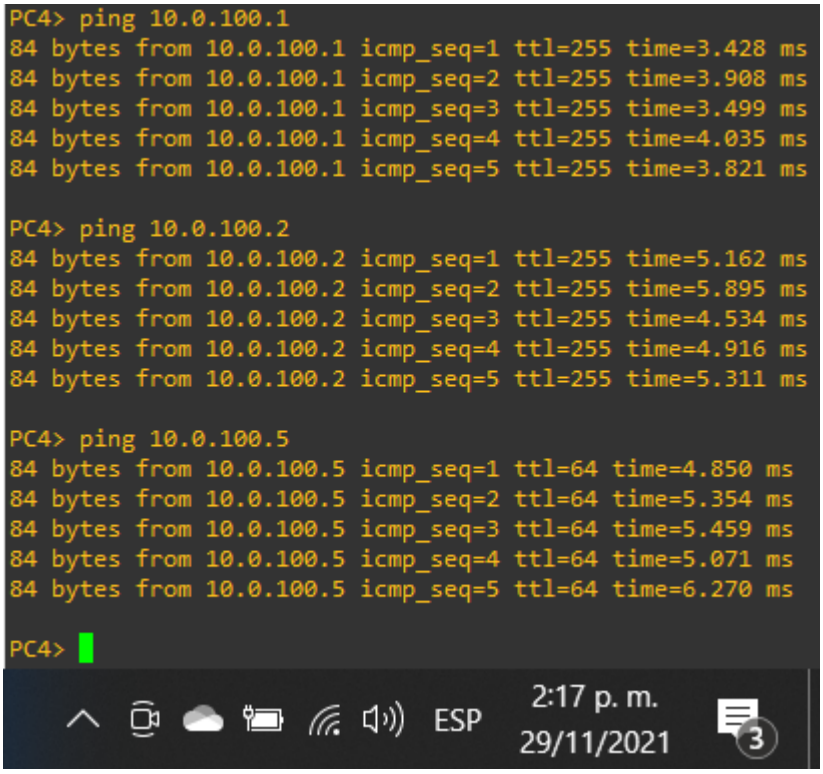
	Figura 6. Verificación de la conectividad en la LAN local en PC2.  	
	Verifique la conectividad de la LAN local.	PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2

Figura 7. Verificación de la conectividad en la LAN local en PC3.



	Verifique la conectividad de la LAN local.	PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5
	Figura 8. Verificación de la conectividad en la LAN local en PC4. 	

Comandos empleados en la parte 2.

Switch D1.

```
D1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface range e0/1-3, e1/0
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range e2/1-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface e2/3
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on Ethernet2/3 but will only
have effect when the interface is in a non-trunking mode.
D1(config-if)#no shutdown
D1(config-if)#exit
```

Switch D2.

```
D2#
D2#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#interface range e0/1-3, e1/0
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D2(config-if-range)#
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface range e2/1-2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#!
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#!
D2(config)#interface e2/3
D2(config-if)#switchport mode Access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet2/3 but will only
have effect when the interface is in a non-trunking mode.
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#end
```

Switch A1

```
A1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range e0/3, e1/0
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface e2/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface e3/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#end
```

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.

Comandos utilizados en cada tarea.

Tabla 5. Las tareas de configuración de la parte 3.

Tarea.	Tarea.	Especificación.
3.1	Comandos	Información para configurar cada dispositivo.
	En R1	
	en conf term router ospf 4 router-id 0.0.4.1	Use OSPF **4** y asigne los siguientes valores id 0.0.4.1

	En R3	
	en conf term router ospf 4 router-id 0.0.4.3	Use OSPF **4** y asigne el siguiente valor id 0.0.4.3.
	En D1	
	config t router ospf 4 router-id 0.0.4.131	Use OSPF **4** y asigne el siguiente valor id 0.0.4.131.
	En D2	
	config t router ospf 4 router-id 0.0.4.132	Use OSPF **4** y asigne el siguiente valor id 0.0.4.132.

	En R1	
	do show ip route connected network 10.0.10.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0 default-information originate exit	En R1 anuncie todas las redesdirectamente conectadas en área 0.
	R3	
	do show ip route connected network 10.0.11.0 0.0.0.255 area 0 network 10.0.13.0 0.0.0.255 area 0 default-information originate exit	En R3 anuncie todas las redesdirectamente conectadas en área 0.

	En D1	
	do show ip route connected 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	En D1 anuncie todas las redesdirectamente conectadas en área 0.
	En D2	
	do show ip route connected 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 10.0.11.0 0.0.0.255 area 0	En D2 anuncie todas las redesdirectamente conectadas en área 0.

	passive-interface default no passive-interface e1/1 passive-interface default no passive-interface e1/1	Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto e1/1. • D2: todas las interfaces excepto e1/1.

Tabla 6. Continuación de la configuración parte 3.

Tarea.	Comandos.	Especificación.
3.2	Comandos	Información para configurar cada dispositivo.
	En R1	
	en conf term router ospf 6 router-id 0.0.6.1	Use OSPF **6** y asigne el siguiente valor id 0.0.6.1
	En R3	
	en conf term router ospf 4 router-id 0.0.6.3	Use OSPF **6** y asigne el siguiente valor id 0.0.6.3
	En D1	
	config t router ospf 4 router-id 0.0.6.131	Use OSPF **6** y asigne el siguiente valor id 0.0.6.131.

	En D2	
	config t router ospf 4 router-id 0.0.6.132	Use OSPF **6** y asigne el siguiente valor id 0.0.6.132
	En R1	
	ipv6 unicast-routing ipv6 router ospf 6 router-id 0.0.6.1 default-information originate exit int g1/0 ipv6 ospf 6 area 0 exit int s3/0 ipv6 ospf 6 area 0 exit	Habilite el enrutamiento IPv6. En R1 anuncie todas las redesdirectamente conectadas a las VLANS en área 0.

	R3	
	ipv6 unicast-routing ipv6 router ospf 6 router-id 0.0.6.3 exit interface g2/0 ipv6 ospf 6 area 0 exit int s1/0 ipv6 ospf 6 area 0 exit exit	Habilite el enrutamiento IPv6. En R3 anuncie todas las redesdirectamente conectadas a las VLANS en área 0.
	En D1.	
	interface e1/1 ipv6 ospf 6 area 0 inter vlan100 ipv6 ospf 6 area 0 inter vlan101 ipv6 ospf 6 area 0 inter vlan102 ipv6 ospf 6 area 0	En D1 anuncie todas las redesdirectamente conectadas a las VLANS en área 0.

	En D2	
	interface e1/1 ipv6 ospf 6 area 0 ipv6 ospf 6 area 0 interface vlan100 ipv6 ospf 6 area 0 interface vlan101 ipv6 ospf 6 area 0 interface vlan102 ipv6 ospf 6 area 0 exit	En D2 anuncie todas las redesdirectamente conectadas a las VLANS en área 0.
	interface e1/1 interface e1/1	Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto e1/1. • D2: todas las interfaces excepto e1/1.

Tabla 7. Finalización de la parte 3.

Tarea.	Comandos.	Especificación.
3.3	Comandos	Información para configurar cada dispositivo.
	En R2 en la “Red ISP”, configure MP-BGP.	
	enable conf term ip route 0.0.0.0 0.0.0.0 loopback 0 ipv6 route ::/0 loopback 0 router bgp 500 bgp router-id 2.2.2.2 neighbor 209.165.200.225 remote-as 300 neighbor 2001:db8:200::1 remote-as 300 address-family ipv4 unicast network 2.2.2.2 mask 255.255.255.255 network 0.0.0.0 mask 0.0.0.0 address-family ipv6 unicast network	Configure dos rutas estáticas interfaz Loopback 0. Configure R2 en BGP ASN **500** y use el id 2.2.2.2. Configure y habilite una relación de vecino IPv4 como en IPv6 con R1 en ASN 300. En IPv4 anuncie la red loopback 0 IPv4 2.2.2.2/32. La ruta por defecto 0.0.0.0/0. En IPv6 anuncie la red

	2001:db8:200::1/128 network ::/0	2001:db8:200::1/128. La ruta por defecto (::/0).
	En R1 en la “Red ISP”, configure MP-BGP.	
3.4	Enable configure terminal ip route 10.0.0.0 255.255.255.0 null 0 router bgp 300 bgp router-id 1.1.1.1 neighbor 209.165.200.226 remote-as 500 address-family ipv4 unicast address-family ipv6 unicast network 2001:db8:200::1/128	Configure 10.0.0.0/8 como Null 0. Configure BGP ASN 300 y use el id 1.1.1.1. Configure una relación de vecino IPv4 como en IPv6 con R2 en ASN 500. Habilite la relación de vecino IPv6 e IPv6. Anuncie la red.

Parte 4:

Configurar la Redundancia del Primer Salto.

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

Tabla 8. Tareas de configuración de la parte 4.

Tarea.	Comandos.	Especificación.
	En D1, cree IP SLAS que prueben la accesibilidad dela interfaz R1 G1/0.	
4.1	configure terminal ip sla 4 icmp-echo 10.0.10.1 frequency 5 exit ip sla schedule 4 start-time now life forever track 4 ip sla 4 state delay up 10 down 15 exit	Use la SLA número **4** para IPv4. Las IP SLAS probarán la disponibilidad de la interfaz R1 G1/0 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización.

	ip sla 6 icmp-echo 2001:db8:100:1010::1 frequency 5 exit ip sla schedule 4 life forever start-time now ip sla schedule 6 life forever start-time now track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit	Cree una IP SLA objeto para la IP SLA 4. Use la SLA número **6** para IPv6. Programe la SLA para una implementación de inicio ahora. Use el número de rastreo **4** para la IP SLA 4. Use el número de rastreo **6** para la IP SLA 6. Notificar a D2 si el estadode IP SLA después de 10 s, o después de 15 segundos.

	En D2, cree IP SLAS que prueben la accesibilidad de la interfaz R3 G2/0.	
4.2	conf term ip sla 4 icmp-echo 10.0.11.1 frequency 5 exit ip sla 6 icmp-echo 2001:db8:100:1011::1 frequency 5 exit ip sla schedule 4 life forever start-time now ip sla schedule 6 life forever start-time now track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit	Use la SLA número **4** para IPv4. Las IP SLAS probarán la disponibilidad de la interfaz R3 G1/0 cada 5 segundos. Use la SLA número **6** para IPv6. Programe la SLA para una implementación de inicio ahora. Use el número de rastreo **4** para la IP SLA 4. Use el número de rastreo **6** para la IP SLA 6. Notificar a D2 si el estado de IP SLA después de 10 s, o después de 15 segundos.

Tabla 9. Continuación de la parte 4.

Tareas y comandos.	**Especificación.**
4.3	En D1 configure HSRPv2. D2 es el router primario para la VLANS 100 y 102; por lo tanto, suprioridad también se cambiará a 150.
interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 priority 150 standby 104 preempt standby 104 track 4 decrement 60	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.

interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 preempt standby 114 track 4 decrement 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.
interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 priority 150 standby 124 preempt standby 124 track 4 decrement 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.

standby 106 ipv6 autoconfig standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 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.
standby 116 ipv6 autoconfig standby 116 priority 150 standby 116 preempt standby 116 track 6 decrement 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.

standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 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.

Tabla 10. Finalización de la parte 4.

Tareas y comandos.	Especificación.
4.3	En D2, configure HSRPv2. D2 es el router primario para la VLAN 101; por lo tanto, suprioridad también se cambiará a 150. Configure HSRP como versión 2.
interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 track 4 decrement 60	Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Habilite la preferencia PREEMPTION. • Rastree el objeto 4 y decremente en 60.

	Configure IPv4 HSRP grupo **114** para la VLAN 101:
interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 priority 150 standby 114 preempt	• Asigne la dirección IP virtual **10.0.101.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia PREEMPTION. • Rastree el objeto 4 para disminuir en 60.
	Configure IPv4 HSRP grupo **124** para la VLAN 102:
interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60	• Asigne la dirección IP virtual **10.0.102.254**. • Habilite la preferencia PREEMPTION. • Rastree el objeto 4 para disminuir en 60.

	Configure IPv6 HSRP grupo **106** para la VLAN 100:
standby 106 ipv6 autoconfig	• Asigne la dirección IP virtual usando **IPV6 AUTOCONFIG**.
standby 106 preempt	• Habilite la preferencia PREEMPTION.
standby 106 track 6 decrement 60	• Rastree el objeto 6 para disminuir en 60.
	Configure IPv6 HSRP grupo **116** para la VLAN 101:
standby 116 ipv6 autoconfig	• Asigne la dirección IP virtual usando **IPV6 AUTOCONFIG**.
standby 116 priority 150	• Establece la prioridad del grupo en **150**.
standby 116 preempt	• Habilite la preferencia PREEMPTION.
standby 116 track 6 decrement 60	• Rastree el objeto 6 para disminuir en 60.

standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60	Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **IPV6 AUTOCONFIG**. • Habilite la preferencia PREEMPTION. • Rastree el objeto 6 para disminuir en 60.

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:

Tabla 11. Configuraciones de parte 5.

Tarea.	Comandos.	Especificación.
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo SCRYPT.	Contraseña: **cisco12345cisco.**
	En R1, R3, D1, D2 y A1.	
	conf term enable password cisco12345cisco service password-encryption	Habilito cisco12345cisco como contraseña. Uso el algoritmo SCRYPT.

	En R1, R3, D1, D2 y A1.	
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de SCRYPT.	Con nombre de usuario local: **SADMIN,** nivel de privilegio **15** y contraseña: **CISCO12345CISCO**
	En R1, R3, D1, D2 y A1.	
	config t enable secret level 15 cisco12345cisco username sadmin privilege 15 secret cisco12345cisco	Nivel de privilegio. Nombre de usuario.
	En R1, R3, D1, D2 y A1	
5.3	En todos los dispositivos (excepto R2),habilite AAA.	Habilite AAA.
	aaa new-model	Habilite AAA en todos menos en R2.

	En R1, R3, D1, D2 y A1.	
5.4	En todos los dispositivos (excepto R2),configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS**.**
	En R1, R3, D1, D2 y A1.	
	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass	Para habilitar AAA se necesita el nombre del servidor. Dirección IP del servidor RADIUS es 10.0.100.6. Numero de puerto UDP 1812 y 1813. Contraseña: **$TRONGPASS.**

	En R1, R3, D1, D2 y A1.	
5.5	En todos los dispositivos (excepto R2),configure la lista de métodos de autenticación AAA.	Especificaciones de autenticación AAA.
	En R1, R3, D1, D2 y A1.	
	config t aaa authentication login default group radius local end	Use la lista de métodos por defecto. Valide con el servidor local.
	En R1, R3, D1, D2 y A1.	
5.6	Verifique el servicio AAA en todos losdispositivos.	Cierre e inicie sesión en todos los dispositivos.

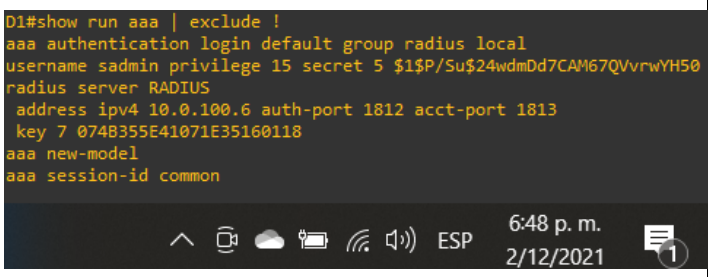
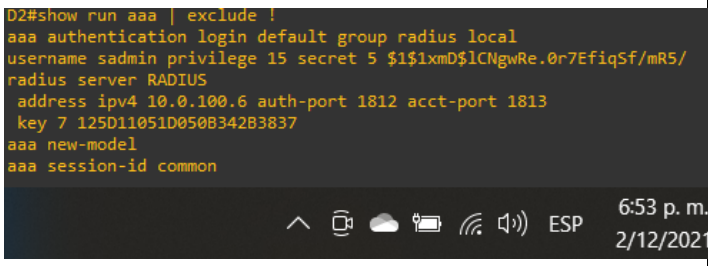
	En R1, R3, D1, D2 y A1.
Figura 9. Comando para verificar esta configuracion en D1.  Figura 10. Comando para verificar esta configuracion en D2.  	Inicie sesión en todos los dispositivos.

Figura 11. Comando para verificar esta configuracion en A1.

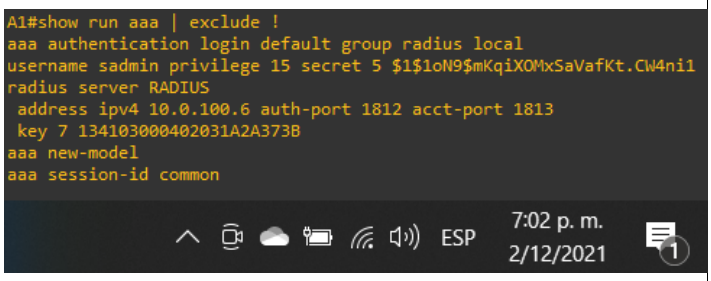


Figura 12. Comando para verificar esta configuracion en R1.

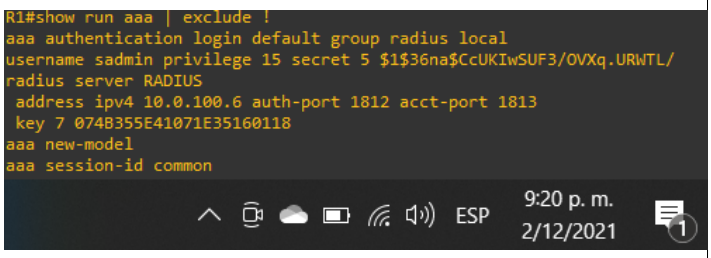
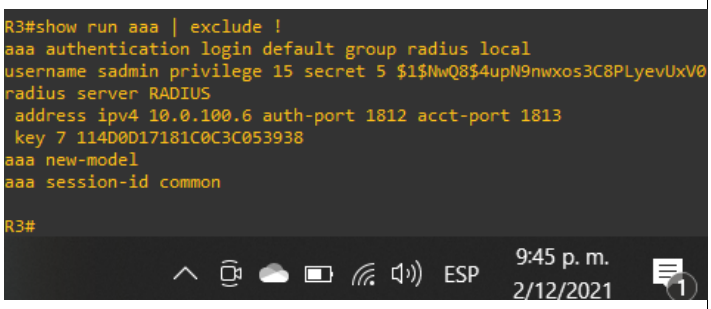
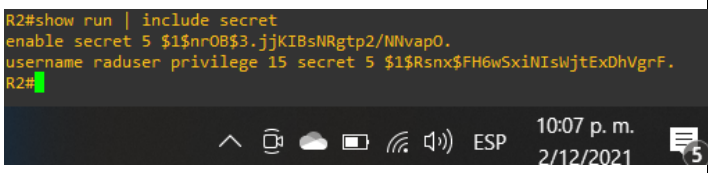


Figura 13. Comadno para verificar esta configuracion en R3.



En R2 con el usuario: **raduser** y la contraseña: **upass123**.

Figura 14. En R2.



Parte 6.

Configure las funciones de Administración de Red.

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

Tabla 12. Las configuraciones de la parte 6.

Tarea.	Comandos.	Especificación.
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
	En R1, R2, R3, D1, D2 y A1.	
	show clock clock set 23:20:00 29 Nov 2021	Muestra el reloj. Ajustar reloj.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.

	En R2.	
	ntp master 3	Configuración de R2 como NTP maestro en el nivel de estrato 3.

Tabla 13. Continuación de la parte 6.

Tarea.	Comandos.	Especificación.
6.3	Configure NTP en R1, R3, D1, D2,y A1.	R1 debe sincronizar con R2. R3, D1 y A1 para sincronizar la hora con R1. D2 para sincronizar la hora con R3.
	Configure NTP en R1.	
	ntp server 2.2.2.2	• R1 debe sincronizar con R2.
	Configure NTP en R3, D1,y A1	
	ntp server 10.0.10.1	En R3, D1 y A1 para sincronizar la hora con R1.
	Configure NTP en D2.	
	ntp server 10.0.10.1	En D2 para sincronizar la hora con R3.
6.4	Configure SYSLOG en todos losdispositivos excepto R2	Los mensajes deben enviarse al PC1 en 10.0.100.5 enel nivel WARNING.

	En R1, R3, D1, D2 y A1.	
	logging trap warning logging host 10.0.100.5 logging on	Especifica un nivel. Habilita la mensajería SYSLOG. Comienza a envía mensajes de SYSLOG.
	En R3, D1 y D2.	
6.5	ip acc ess-list standard SNMP-NMS permit host 10.0.100.5 exit snmp-server contact VictorR snmp-server community ENCORSA ro SNMP-NMS snmp-server host 10.0.100.5 version 2c ENCORSA snmp-server enable traps config snmp-server enable traps ospf	Limite el acceso SNMP. dirección IP de laPC1. Configure el valor de contacto SNMP con sunombre. Establece la comunidad en **ENCORSA**. Configura esta cadena. Habilite el envío de TRAPS: CONFIG y OSPF.

	En R1	
	ip access-list standard SNMP-NMS	Limite el acceso SNMP.
	permit host 10.0.100.5	Dirección IP de la PC1.
	exit	
	snmp-server contact Cisco VictorR	Configure el valor de contacto SNMP con su nombre.
	snmp-server community ENCORSA ro SNMP-NMS	
	snmp-server host 10.0.100.5 versión 2c ENCORSA	Establece la comunidad en **ENCORSA**.
	snmp-server ifindex persist	Configura esta cadena.
	snmp-server enable traps bgp	
	snmp-server enable traps config	
	snmp-server enable traps ospf	Habilita globalmente la persistencia de IFINDEX de SNMP.
	end	Habilite el envío de *TRAPS: BGP, CONFIG y OSP.*

	En A1.	
	ip access-list standard SNMP-NMS permit host 10.0.100.5 exit	Limite el acceso SNMP. Dirección IP de la PC1.
	snmp-server contact VictorR	Configure el valor de contacto SNMP con su nombre.
	snmp-server community ENCORSA ro SNMP-NMS	Establezca la comunidad en **ENCORSA**.
	snmp-server host 10.0.100.5 version 2c ENCORSA	Configura esta cadena.
	snmp-server ifindex persist	Habilita globalmente la persistencia de IFINDEX de SNMP.
	snmp-server enable traps config snmp-server enable traps ospf	En A1, habilite el envío de *TRAPS CONFIG*.

CONCLUSIONES

Aprendí mucho sobre el manejo y todo lo necesario en el software GNS3 para poder diseñar la topología fue necesario lograr vincular gns3 con virtual box.

Observe que en la simulación obtendría más de un archivo ya que la configuración de cada dispositivo no quedaba guardada en la topología si no que se debe guardar de manera individual lo que se realiza en cada dispositivo.

Analicé en el transcurso de la simulación que los routers R1, R2 y R3 se demoran mucho más tiempo en encender que un switch, por lo que esto me llevo más tiempo de lo que se ocupar en Cisco Packet Tracer.

Aplique muchos comandos que suelo emplear en Cisco Packet Tracer, los use en gns3 de forma más rápida porque la mayoría son comandos que hemos manejado mucho lo que me permitieron agilizar y realizar de forma completa la configuración de cada dispositivo.

BIBLIOGRÁFIA

PARRA H. (2021), Web CCNP unidades 8, 9 y 10. Recuperado de https://drive.google.com/file/d/1aHYc08lI27zbypmCBn-r1v_q1WsKE1xs/view

PARRA H. (2021), Web CCNP unidades 8, 9 y 10. Recuperado de https://drive.google.com/file/d/1aHYc08lI27zbypmCBn-r1v_q1WsKE1xs/view

STUDY-CCNA.COM. (2021). IEEE 802.1Q. Recuperado de https://study-ccna.com/ieee-802-1q/

STUDY-CCNA.COM. (2021). ¿Qué es IPv6? Recuperado de https://study-ccna.com/what-is-ipv6/

STUDY-CCNA.COM. (2021). ¿Qué es STP? Recuperado de https://study-ccna.com/what-is-stp/

STUDY-CCNA.COM. (2021). ¿Qué es la dirección IPv4 y cuál es su función en la red? Asignación de direcciones IPv4. Estático. Recuperado de https://study-ccna.com/what-is-ipv4-address/

STUDY-CCNA.COM. (2021). ¿Qué es la dirección IPv4 y cuál es su función en la red? Asignación de direcciones IPv4. Dinámico. Recuperado de https://study-ccna.com/what-is-ipv4-address/