

INFORME – PRUEBA DE HABILIDADES PRÁCTICA

JOSE RAFAEL LLANES PIZARRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2022

INFORME – PRUEBA DE HABILIDADES PRÁCTICA

JOSE RAFAEL LLANES PIZARRO

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

DIRECTOR

Ing. JOHN HAROLD PEREZ CALDERON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2022

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 30 de noviembre de 2022

AGRADECIMIENTOS

Le agradezco a todas las personas que interviene en este proyecto, mi familia que me inspira a seguir adelante, la gran ayuda brindada por todos los tutores y me acompañaron en la carrera que con gran esfuerzo cumplimos a cabalidad, que el objetivo principal entre nosotros era brindarnos ayuda y conocimiento en el área en las cuales tuvimos dificultades.

Inmensas gracias le quiero dar a mi esposa, la cual me apoyo cada día en este largo proceso y que con su amor me fortalecía día, tras día, a mis padres les dedico este logro de mi vida y espero los haga sentir muy orgullosos.

Muchas Gracias, por ser parte del proceso.

CONTENIDO

GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT	9
INTRODUCCIÓN.....	10
ESCENARIO	11
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES.....	11
Paso 1: Cablear la red como se muestra en la topología.....	11
TABLA DE DIRECCIONAMIENTO	12
Paso 2: Configurar los parámetros básicos para cada dispositivo	12
EVIDENCIA DE LA CONFIGURACION PARTE 1	20
PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST.....	21
Paso 1: Configurar las interfaces troncales.....	21
Paso 2: Configurar la VLAN 99 como nativa	21
Paso 3: Habilitar protocolo Rapid Spanning-Tree (RSTP).	22
Paso 4: Configurar los puentes raíz (root bridges).....	23
Paso 5: crear los LACP.....	24
Paso 6: Configurar los puertos de acceso a los PC.	26
Paso 7: Verificar los PC en DHCP	27
Paso 8: Verificación de la conectividad de la LAN local	27
PART 3 CONFIGURE ROUTING PROTOCOLS	30
Paso 1 Configuración OSPFv2	30
Paso 2: Configuración de OSPFv3	31
Paso 3: Configuración MP-BGP en la red ISP R2.....	32
Paso 4: Configuración MP-BGP en la red ISP R1.....	33
EVIDENCIAS DE CONFIGURACION PARTE 3.....	34
Paso 5: Verificación del MP-BGP con Ping.....	38
PART 4 CONFIGURE FIRST HOP REDUNDANCY	39
Paso 1: En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.....	39
Paso 2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.....	39
Paso 3: En D1 configure HSRPv2.....	40
Paso 4: En D2 configure HSRPv2.	41
EVIDENCIAS DE CONFIGURACION PARTE 4.....	42
CONCLUSIONES.....	45
BIBLIOGRAFÍA.....	46

LISTA DE TABLAS

Tabla 1.	Direccionamiento IP.....	12
----------	--------------------------	----

LISTA DE FIGURAS

Figura 1. Montaje del escenario propuesto.	11
Figura 2. Configuración de IP en los PC.....	20
Figura 3. Verificación de los enlaces troncales.....	22
Figura 4. Verificación de spanning-tree	23
Figura 5. Verificación del LACP	27
Figura 6. IP de los PC en DHCP	27
Figura 7. Ping entre los dispositivos de la red local.....	29
Figura 8. Verificación de show run section ^router ospf on R1, R3, D1, and D2.....	34
Figura 9. Verificación show run section ^ipv6 router and show ipv6 ospf.....	35
Figura 10. Verificación show run section bgp and show run include route on R2.....	36
Figura 11. Verificación show run section bgp on R1.....	36
Figura 12. Verificación show ip route include O B on R1.....	36
Figura 13. Verificación show ipv6 route command on R1.....	37
Figura 14. Verificación de show ip route ospf begin Gateway	37
Figura 15. Verificación show ipv6 route ospf command on R3.....	37
Figura 16. Verificación de la tabla de ruta IPv4	38
Figura 17. Verificación de Ping D1 y D2 hacia Loopback 0.....	38
Figura 18. Verificación de show run section ip sla.....	42
Figura 19. Verificación de show standby brief command on D1 y D2.....	43
Figura 20. Verificación de show run section ip sla command on D1 -D2.....	43
Figura 21. Verificación de Verificación del Standby	44

GLOSARIO

ASN: *Autonomous System Number*, se le denomina al grupo de red que es gestionado por algún operador de red por ruteo externo.

BGP: *Border Gateway Protocol*, utilizado para conectar distintos sistemas autónomos principalmente con el canal de internet.

DHCP: *Dynamic Host Configuration Protocol*, funciona en el modelo cliente/servidor y proporciona automáticamente direcciones IP y otra información relacionada como la máscara y el Gateway.

HSRP: *Host Standby Routing Protocol*, asigna a un grupo de redundancia un router activo, otro standby y los demás en estado listen, donde el activo tendrá la IP virtual.

ISP: *Internet Service Provider*, término que identifica las compañías que proveen acceso a internet.

LACP: *Link Agregation Control Protocol*, característico de la capa 2 une puertos físicos de la red en un único puerto lógico de gran ancho de banda, y crea redundancias.

RESUMEN

A continuación se desarrolla este documento, enfocado a las habilidades prácticas del curso, proyectándose como opción de grado en la carrera de ingeniería en telecomunicaciones, se desarrollan las habilidades prácticas CCNP en los entornos o escenarios según la guía de actividades, se muestra la simulación en GNS3 manejando las herramientas e imágenes IOS de los elementos de CISCO, realizar las configuraciones de diferentes equipos como switches, routers, pc, de esta forma se mide las capacidades, cualidades y conocimientos de los estudiantes en la ingeniería de telecomunicaciones. Se configuran los protocolos de comunicación, enrutamientos, redes necesarias y todos los equipos de comunicación

Palabras clave: Enrutamiento, Redes, CISCO, CCNP, Conmutación, GNS3, IOS.

ABSTRACT

This document is developed below, focused on the practical skills of the course, projecting itself as a degree option in the telecommunications engineering career, CCNP practical skills are developed in the environments or scenarios according to the activity guide, the simulation is shown in GNS3 managing the IOS tools and images of the CISCO elements, making the configurations of different equipment such as switches, routers, PC, in this way the capacities, qualities and knowledge of the students in telecommunications engineering are measured. Communication protocols, routing, necessary networks and all communication equipment are configured

Key words: Routing, Networks, CISCO, CCNP, Switching, GNS3, IOS

INTRODUCCIÓN

En el desarrollo de este trabajo se relaciona las telecomunicaciones dependiendo de la guía de actividades propuestas en el curso, como ingeniero de telecomunicaciones es de gran importancia facilitar el proceso de las telecomunicaciones, el aprendizaje del día a día de este medio, mostrar las mejoras y los nuevos medios tecnológicos que van saliendo, como es la interacción entre los equipos de comunicación, personas, empresas y los medios remotos de operar estos elementos.

Como ingeniero en Telecomunicaciones se aplicará el conocimiento de conexión y configuración de los equipos de comunicaciones, con esto se desarrolla los ejercicios den GNS3, Cisco Packet Tracer, etc. en este escenario se muestra, 3 router, 3 switches y 4 PCs, haciendo la simulación respectiva del mismo, direccionamiento en los dispositivos IPv6, IPv4 Swiches, utilizado RSTP Rapid y enlaces LACP.

ESCENARIO

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.

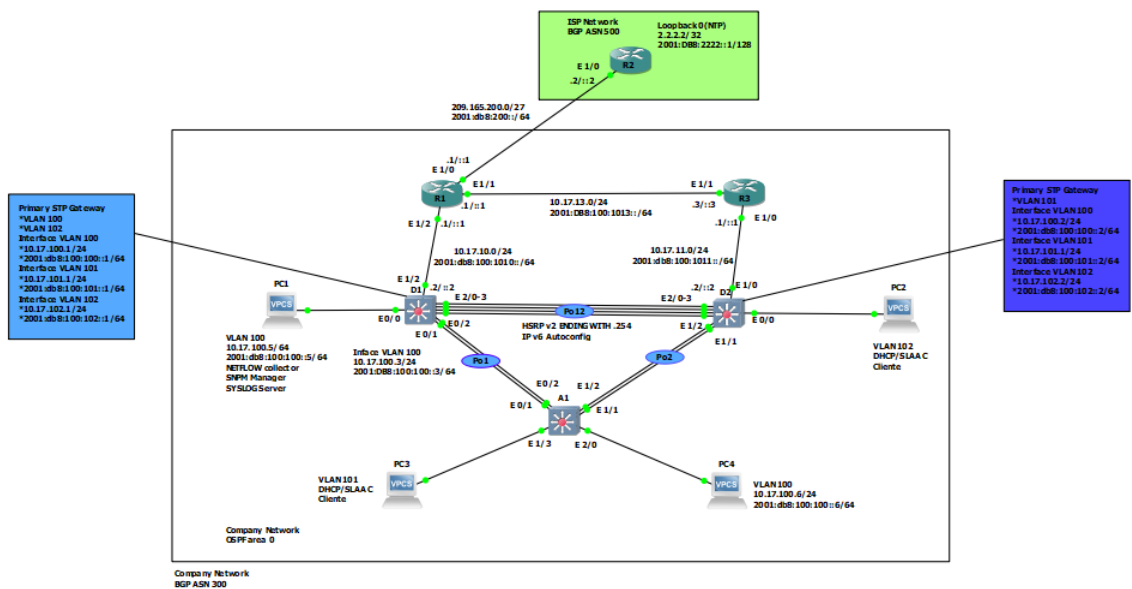


Figura 1. Montaje del escenario propuesto.

TABLA DE DIRECCIONAMIENTO

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local	
	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.17.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
R1	E1/1	10.17.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
R2	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
	E1/0	10.17.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
R3	E1/1	10.17.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
	E1/2	10.17.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.17.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.17.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
D1	VLAN 102	10.17.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
	E1/0	10.17.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.17.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.17.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
D2	VLAN 102	10.17.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.17.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.17.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64

Tabla 1. Direccionamiento IP

Paso 2: Configurar los parámetros básicos para cada dispositivo

Se procede a configurar los parámetros básicos de los dispositivos como los nombres, textos de banner para cada equipo, específicamente las IP de cada interfaz tanto en IPV4 como en IPV6 de cada uno de los router, en el caso de los switches la creación de las VLAN con sus nombres, las direcciones IP, y se crea un pool DHCP con sus respectivas exclusiones.

Router 1:

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
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 e1/2
ip address 10.17.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface e1/1
ip address 10.17.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
Destination filename [startup-config]? Building configuration...
[OK]R1#
```

Router 2:

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
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 3:

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
interface e1/0
ip address 10.17.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface e1/1
ip address 10.17.13.3 255.255.255.0
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#
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 e1/2
no switchport
ip address 10.17.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.17.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.17.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.17.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.17.101.1 10.0.101.109
ip dhcp excluded-address 10.17.101.141 10.0.101.254
```



```
ip dhcp excluded-address 10.17.102.1 10.0.102.109
ip dhcp excluded-address 10.17.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.17.101.0 255.255.255.0
default-router 10.17.101.254
exit
ip dhcp pool VLAN-102
network 10.17.102.0 255.255.255.0
default-router 10.17.102.254
exit
exit
copy run star
```

Switch D2:

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment#
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 e1/0
no switchport
ip address 10.17.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.17.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.17.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.17.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.17.101.1 10.0.101.209
ip dhcp excluded-address 10.17.101.241 10.0.101.254
```

```
ip dhcp excluded-address 10.17.102.1 10.0.102.209
ip dhcp excluded-address 10.17.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.17.101.0 255.255.255.0
default-router 17.0.101.254
exit
ip dhcp pool VLAN-102
network 10.17.102.0 255.255.255.0
default-router 10.17.102.254
exit
exit
copy run star
```

Switch A1:

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment#
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 10.17.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
exit
copy run star
```

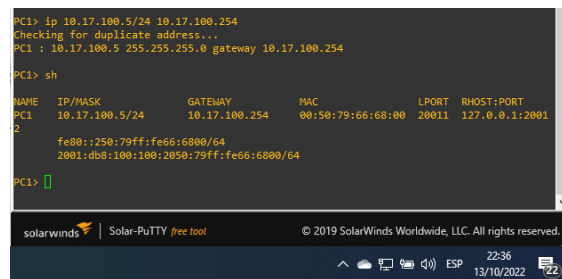
EVIDENCIA DE LA CONFIGURACION PARTE 1

```
PC1> ip 10.17.100.5/24 10.17.100.254
Checking for duplicate address...
PC1 : 10.17.100.5 255.255.255.0 gateway 10.17.100.254

PC1> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.17.100.5/24 10.17.100.254 00:50:79:66:68:00 20011 127.0.0.1:2001
2
fe80::250:79ff:fe66:6800/64
2001:db8:100:100:2050:79ff:fe66:6800/64

PC1> █
```



```
PC4> ip 10.17.100.6/24 10.17.100.254
Checking for duplicate address...
PC4 : 10.17.100.6 255.255.255.0 gateway 10.17.100.254

PC4> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.17.100.6/24 10.17.100.254 00:50:79:66:68:03 20017 127.0.0.1:2001
8
fe80::250:79ff:fe66:6803/64
2001:db8:100:1011:2050:79ff:fe66:6803/64

PC4> █
```

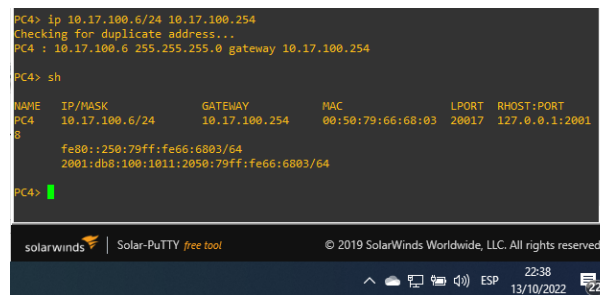


Figura 2. Configuración de IP en los PC

PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST

Paso 1: Configurar las interfaces troncales

Switch D1:

```
interface range e2/0 - 3, e0/1 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

Switch D2:

```
interface range e2/0 - 3, e1/1 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Switch A1:

```
interface range e0/1 - 2
switchport trunk encapsulation dot1q
switchport mode trunk
```

Paso 2: Configurar la VLAN 99 como nativa

Switch D1:

```
interface range e2/0 - 3, e0/1 - 2
switchport trunk native vlan 999
```

Switch D2:

```
interface range e2/0 - 3, e1/1 - 2
```

switchport trunk native vlan 999

Switch A1:

interface range e0/1 – 2

switchport trunk native vlan 999

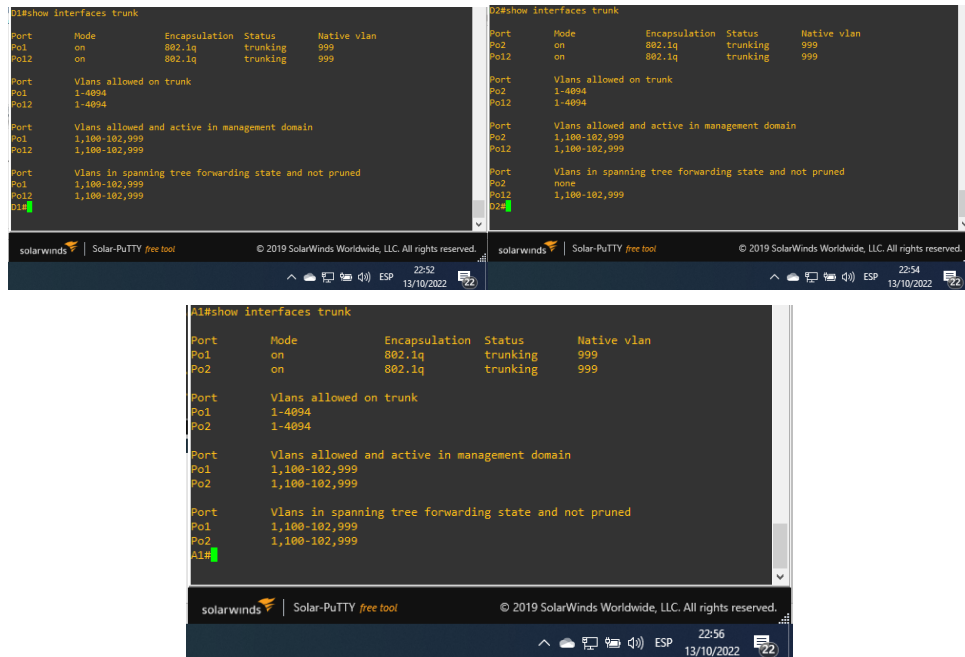


Figura 3. Verificación de los enlaces troncales

Paso 3: Habilitar protocol Rapid Spanning-Tree (RSTP).

Switch D1:

spanning-tree mode rapid-pvst

Switch D2:

spanning-tree mode rapid-pvst

Switch A1:

spanning-tree mode rapid-pvst

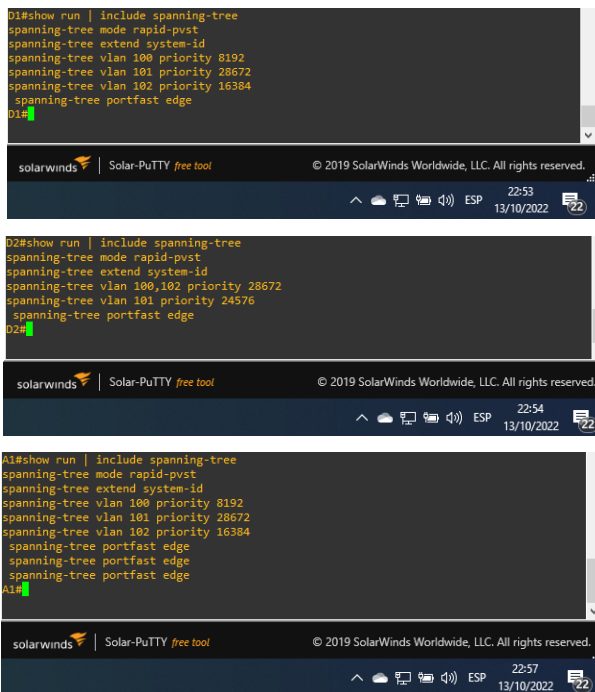
Paso 4: Configurar los puentes raíz (root bridges)

Switch D1:

```
spanning-tree vlan 100 root primary
spanning-tree vlan 102 root primary
spanning-tree vlan 101 root secondary
```

Switch D2:

```
spanning-tree vlan 101 root primary
spanning-tree vlan 100 root secondary
spanning-tree vlan 102 root secondary
```



```
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100 priority 8192
spanning-tree vlan 101 priority 28672
spanning-tree vlan 102 priority 16384
spanning-tree portfast edge
D1#
```

```
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
spanning-tree portfast edge
D2#
```

```
A1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100 priority 8192
spanning-tree vlan 101 priority 28672
spanning-tree vlan 102 priority 16384
spanning-tree portfast edge
spanning-tree portfast edge
spanning-tree portfast edge
A1#
```

Figura 4. Verificación de spanning-tree

Paso 5: crear los LACP.

Switch D1:

```
interface range e2/0-3
channel-protocol lacp
channel-group 12 mode active
Creating a port-channel interface Port-channel 12
exit
interfac port-channel 12
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
exit
interface range e0/1-2
channel-protocol lacp
channel-group 1 mode active
Creating a port-channel interface Port-channel 1
exit
interfac port-channel 1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
exit
```

Switch D2:

```
interface range e2/0-3
channel-protocol lacp
channel-group 12 mode active
Creating a port-channel interface Port-channel 12
```



```
exit
interfac port-channel 12
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
exit
interface range e1/1-2
channel-protocol lacp
channel-group 2 mode active
Creating a port-channel interface Port-channel 2
exit
interfac port-channel 2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
exit
```

Switch A1:

```
interface range e0/1-2
channel-protocol lacp
channel-group 1 mode active
Creating a port-channel interface Port-channel 1
exit
interfac port-channel 1
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
switchport mode trunk
exit
interface range e1/1-2
```

```
channel-protocol lacp
channel-group 2 mode passive
Creating a port-channel interface Port-channel 2
exit
interfac port-channel 2
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
exit
```

Paso 6: Configurar los puertos de acceso a los PC.

Switch D1:

```
interface e0/0
switchport mode access
switchport access vlan 100
```

Switch D2:

```
interface e0/0
switchport mode access
switchport access vlan 102
```

Switch A1:

```
interface e1/3
switchport mode access
switchport access vlan 101
exit
interface e2/0
switchport mode access
switchport access vlan 100
exit
```

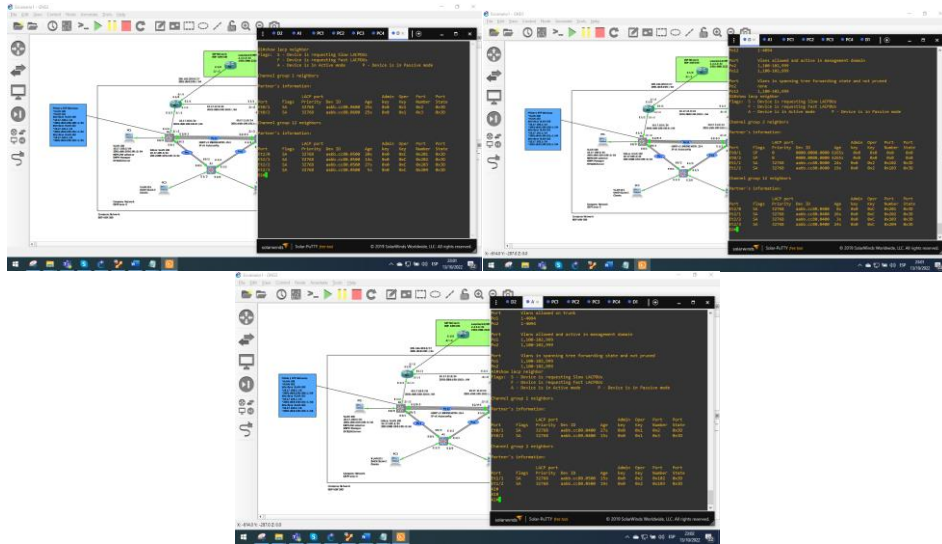


Figura 5. Verificación del LACP

Paso 7: Verificar los PC en DHCP

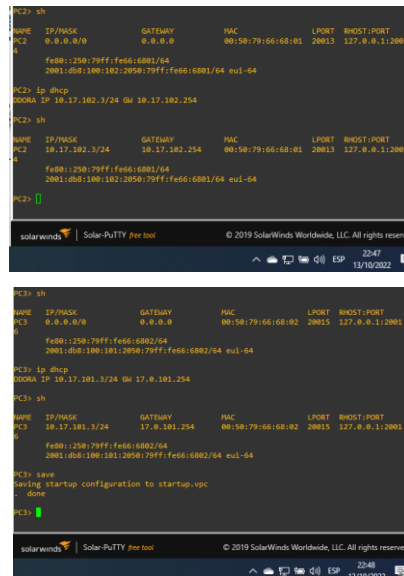


Figura 6. IP de los PC en DHCP

Paso 8: Verificación de la conectividad de la LAN local

PC1 should successfully ping:

- D1: 10.53.100.1
- D2: 10.53.100.2

- PC4: 10.53.100.6

```

PC1> ping 10.17.100.1
Pinging 10.17.100.1 with 32 bytes of data:
84 bytes from 10.17.100.1 icmp_seq=1 ttl=255 time=0.294 ms
84 bytes from 10.17.100.1 icmp_seq=2 ttl=255 time=0.613 ms
84 bytes from 10.17.100.1 icmp_seq=3 ttl=255 time=0.517 ms
84 bytes from 10.17.100.1 icmp_seq=4 ttl=255 time=0.725 ms
84 bytes from 10.17.100.1 icmp_seq=5 ttl=255 time=0.518 ms

PC1> ping 10.17.100.2
Pinging 10.17.100.2 with 32 bytes of data:
84 bytes from 10.17.100.2 icmp_seq=1 ttl=255 time=3.733 ms
84 bytes from 10.17.100.2 icmp_seq=2 ttl=255 time=0.943 ms
84 bytes from 10.17.100.2 icmp_seq=3 ttl=255 time=0.881 ms
84 bytes from 10.17.100.2 icmp_seq=4 ttl=255 time=0.910 ms
84 bytes from 10.17.100.2 icmp_seq=5 ttl=255 time=0.835 ms

PC1> ping 10.17.100.6
Pinging 10.17.100.6 with 32 bytes of data:
84 bytes from 10.17.100.6 icmp_seq=1 ttl=64 time=1.358 ms
84 bytes from 10.17.100.6 icmp_seq=2 ttl=64 time=2.883 ms
84 bytes from 10.17.100.6 icmp_seq=3 ttl=64 time=1.241 ms
84 bytes from 10.17.100.6 icmp_seq=4 ttl=64 time=1.069 ms
84 bytes from 10.17.100.6 icmp_seq=5 ttl=64 time=2.628 ms

PC1>

```

PC2 should successfully ping:

- D1: 10.53.102.1
- D2: 10.53.102.2

```

PC2> ping 10.17.102.1
Pinging 10.17.102.1 with 32 bytes of data:
84 bytes from 10.17.102.1 icmp_seq=1 ttl=255 time=0.740 ms
84 bytes from 10.17.102.1 icmp_seq=2 ttl=255 time=0.851 ms
84 bytes from 10.17.102.1 icmp_seq=3 ttl=255 time=0.985 ms
84 bytes from 10.17.102.1 icmp_seq=4 ttl=255 time=1.268 ms
84 bytes from 10.17.102.1 icmp_seq=5 ttl=255 time=1.080 ms

PC2> ping 10.17.102.2
Pinging 10.17.102.2 with 32 bytes of data:
84 bytes from 10.17.102.2 icmp_seq=1 ttl=255 time=0.395 ms
84 bytes from 10.17.102.2 icmp_seq=2 ttl=255 time=0.641 ms
84 bytes from 10.17.102.2 icmp_seq=3 ttl=255 time=0.647 ms
84 bytes from 10.17.102.2 icmp_seq=4 ttl=255 time=0.545 ms
84 bytes from 10.17.102.2 icmp_seq=5 ttl=255 time=1.042 ms

PC2>

```

PC3 should successfully ping:

- D1: 10.53.101.1
- D2: 10.53.101.2

```

PC3> ping 10.17.101.1
Pinging 10.17.101.1 with 32 bytes of data:
84 bytes from 10.17.101.1 icmp_seq=1 ttl=255 time=0.792 ms
84 bytes from 10.17.101.1 icmp_seq=2 ttl=255 time=1.071 ms
84 bytes from 10.17.101.1 icmp_seq=3 ttl=255 time=1.013 ms
84 bytes from 10.17.101.1 icmp_seq=4 ttl=255 time=0.808 ms
84 bytes from 10.17.101.1 icmp_seq=5 ttl=255 time=1.296 ms

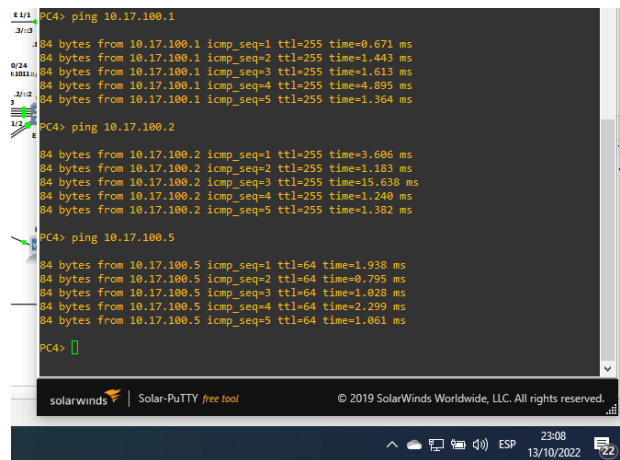
PC3> ping 10.17.101.2
Pinging 10.17.101.2 with 32 bytes of data:
84 bytes from 10.17.101.2 icmp_seq=1 ttl=255 time=1.158 ms
84 bytes from 10.17.101.2 icmp_seq=2 ttl=255 time=1.737 ms
84 bytes from 10.17.101.2 icmp_seq=3 ttl=255 time=1.295 ms
84 bytes from 10.17.101.2 icmp_seq=4 ttl=255 time=1.325 ms
84 bytes from 10.17.101.2 icmp_seq=5 ttl=255 time=1.238 ms

PC3>

```

PC4 should successfully ping:

- D1: 10.53.100.1
- D2: 10.53.100.2
- PC1: 10.53.100.5



```
PC4> ping 10.17.100.1
84 bytes from 10.17.100.1 icmp_seq=1 ttl=255 time=0.671 ms
84 bytes from 10.17.100.1 icmp_seq=2 ttl=255 time=1.443 ms
84 bytes from 10.17.100.1 icmp_seq=3 ttl=255 time=1.613 ms
84 bytes from 10.17.100.1 icmp_seq=4 ttl=255 time=4.895 ms
84 bytes from 10.17.100.1 icmp_seq=5 ttl=255 time=1.364 ms

PC4> ping 10.17.100.2
84 bytes from 10.17.100.2 icmp_seq=1 ttl=255 time=3.606 ms
84 bytes from 10.17.100.2 icmp_seq=2 ttl=255 time=1.183 ms
84 bytes from 10.17.100.2 icmp_seq=3 ttl=255 time=15.638 ms
84 bytes from 10.17.100.2 icmp_seq=4 ttl=255 time=1.240 ms
84 bytes from 10.17.100.2 icmp_seq=5 ttl=255 time=1.382 ms

PC4> ping 10.17.100.5
84 bytes from 10.17.100.5 icmp_seq=1 ttl=64 time=1.938 ms
84 bytes from 10.17.100.5 icmp_seq=2 ttl=64 time=0.795 ms
84 bytes from 10.17.100.5 icmp_seq=3 ttl=64 time=1.028 ms
84 bytes from 10.17.100.5 icmp_seq=4 ttl=64 time=2.299 ms
84 bytes from 10.17.100.5 icmp_seq=5 ttl=64 time=1.061 ms

PC4> |
```

Figura 7. Ping entre los dispositivos de la red local

PART 3 CONFIGURE ROUTING PROTOCOLS

Paso 1 Configuración OSPFv2

Router R1:

```
router ospf 4
router-id 0.0.4.1
network 10.17.10.0 0.0.0.255 area 0
network 10.17.13.0 0.0.0.255 area 0
exit
ip route 0.0.0.0 0.0.0.0 e1/0
router ospf 4
default-information originate
```

Router R3:

```
router ospf 4
router-id 0.0.4.3
network 10.17.11.0 0.0.0.255 area 0
network 10.17.13.0 0.0.0.255 area 0
```

Switch D1:

```
router ospf 4
router-id 0.0.4.131
network 10.17.10.0 0.0.0.255 area 0
network 10.17.100.0 0.0.0.255 area 0
network 10.17.101.0 0.0.0.255 area 0
network 10.17.102.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/2
```

Switch D2:

```
router ospf 4
router-id 0.0.4.132
network 10.17.11.0 0.0.0.255 area 0
network 10.17.100.0 0.0.0.255 area 0
network 10.17.101.0 0.0.0.255 area 0
network 10.17.102.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/0
```

Paso 2: Configuración de OSPFv3**Router R1:**

```
ipv6 router ospf 6
router-id 0.0.6.1
exit
interface e1/1
ipv6 ospf 6 area 0
interface e1/2
ipv6 ospf 6 area 0
exit
ipv6 router ospf 6
default-information originate
```

Router R3:

```
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e1/0
ipv6 ospf 6 area 0
interface e1/1
ipv6 ospf 6 area 0
```

Switch D1:

```
ipv6 router ospf 6
router-id 0.0.6.131
interface e1/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
interface vlan 101
ipv6 ospf 6 area 0
interface vlan 102
ipv6 ospf 6 area 0
```

Switch D2:

```
ipv6 router ospf 6
router-id 0.0.6.132
interface e1/0
ipv6 ospf 6 area 0
interface vlan 100
ipv6 ospf 6 area 0
interface vlan 101
ipv6 ospf 6 area 0
interface vlan 102
ipv6 ospf 6 area 0
```

Paso 3: Configuración MP-BGP en la red ISP R2.**Router R2:**

```
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
no bgp default ipv4-unicast
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4 unicast
neighbor 209.165.200.225 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0 mask 0.0.0.0
exit
address-family ipv6 unicast
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::1/128
network ::/0
exit
```

Paso 4: Configuración MP-BGP en la red ISP R1

Router R1:

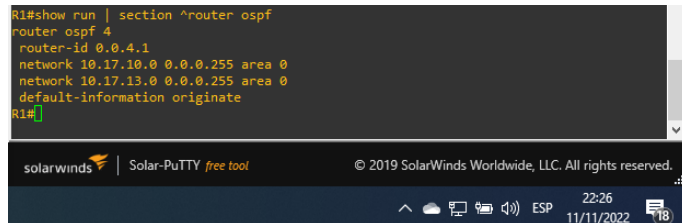
```
ip route 10.0.0.0 255.0.0.0 null 0
ipv6 route 2001:db8:100::/48 null 0
router bgp 300
bgp router-id 1.1.1.1
no bgp default ipv4-unicast
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
network 10.0.0.0 mask 255.0.0.0
exit
address-family ipv6 unicast
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
```

EVIDENCIAS DE CONFIGURACIÓN PARTE 3

Issue show run | section ^router ospf on R1, R3, D1, and D2; output should appear as below. Verify task 3.1 on each device.

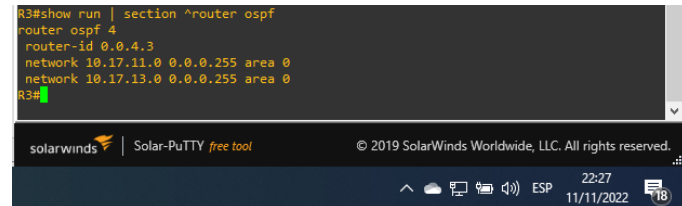
Router R1:

```
R1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
network 10.17.10.0 0.0.0.255 area 0
network 10.17.13.0 0.0.0.255 area 0
default-information originate
R1#
```



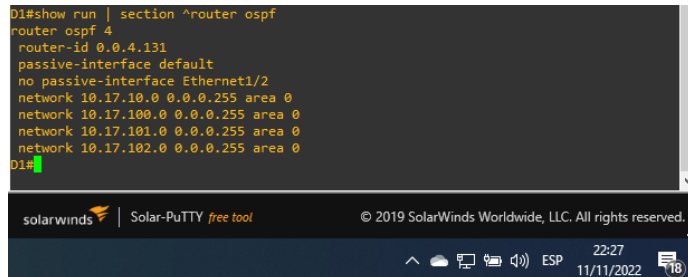
Router R3:

```
R3#show run | section ^router ospf
router ospf 4
router-id 0.0.4.3
network 10.17.11.0 0.0.0.255 area 0
network 10.17.13.0 0.0.0.255 area 0
R3#
```



Switch D1:

```
D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
network 10.17.10.0 0.0.0.255 area 0
network 10.17.100.0 0.0.0.255 area 0
network 10.17.101.0 0.0.0.255 area 0
network 10.17.102.0 0.0.0.255 area 0
D1#
```



Switch D2:

```
D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
network 10.17.11.0 0.0.0.255 area 0
network 10.17.100.0 0.0.0.255 area 0
network 10.17.101.0 0.0.0.255 area 0
network 10.17.102.0 0.0.0.255 area 0
D2#
```

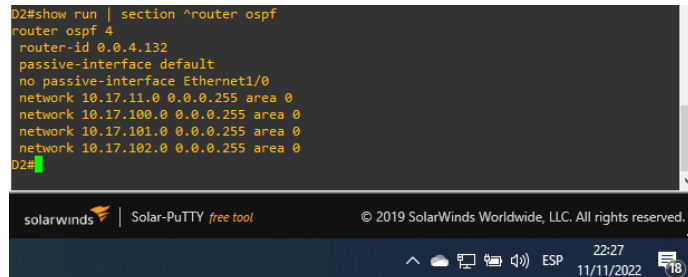


Figura 8. Verificación de show run | section ^router ospf on R1, R3, D1, and D2

Issue show run | section ^ipv6 router and show ipv6 ospf interface brief on R1, R3, D1, and D2; output should appear as below. Verify task 3.2 on each device.

Router R1:

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
Et1/2     6   0     6        10   DR    1/1
Et1/1     6   0     5        10   DR    1/1
R1#
```

Router R3:

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
Et1/1     6   0     5        10   BDR   1/1
Et1/0     6   0     4        10   DR    1/1
R3#
```

Switch D1:

```
D1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
D1#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
V1102     6   0     21        1   BDR   1/1
V1101     6   0     20        1   BDR   1/1
V1100     6   0     19        1   BDR   1/1
Et1/2     6   0     17        10   BDR   1/1
D1#
```

Switch D2:

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.132
D2#show ipv6 ospf interface brief
Interface  PID  Area  Intf ID  Cost  State  Nbrs  F/C
V1102     6   0     21        1   DR    1/1
V1101     6   0     20        1   DR    1/1
V1100     6   0     19        1   DR    1/1
Et1/0     6   0     17        10   BDR   1/1
D2#
```

Figura 9. Verificación show run | section ^ipv6 router and show ipv6 ospf

Issue show run | section bgp and show run | include route on R2; output should appear as below. Verify task 3.3.

Router R2:

```
R2#show run | section bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.226 remote-as 300
}
address-family ipv4
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  neighbor 209.165.200.226 activate
exit-address-family
}
address-family ipv6
  network ::
  network 2001:DB8:2222::1/128
  neighbor 2001:DB8:200::1 activate
exit-address-family
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
  ip route 0.0.0.0 0.0.0.0 Loopback0
ip route ::/0 Loopback0
R2#
```

Figura 10. Verificación show run | section bgp and show run | include route on R2

Issue show run | section bgp on R1; output should appear as below. Verify task 3.4.

Router R1:

```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
}
address-family ipv4
  network 10.17.0.0 mask 255.255.0.0
  neighbor 209.165.200.226 activate
exit-address-family
}
address-family ipv6
  network 2001:DB8:100::/48
  neighbor 2001:DB8:200::2 activate
exit-address-family
R1#
```

Figura 11. Verificación show run | section bgp on R1

Issue show ip route | include O/B on R1; output should appear as below. Verify that OSPF and BGP for IPv4 are working properly.

Router R1:

```
R1#show ip route | include O/B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
o - ODR, P - periodic downloaded static route, H - NHRP, I - ISIS
B 2.2.2.2 [26/0] via 209.165.200.226, 00:14:57
D 10.17.11.0/24 [110/20] via 10.17.10.2, 00:14:17, Ethernet1/1
D 10.17.100.0/24 [110/11] via 10.17.10.2, 00:13:48, Ethernet1/2
D 10.17.101.0/24 [110/11] via 10.17.10.2, 00:13:48, Ethernet1/2
D 10.17.102.0/24 [110/11] via 10.17.10.2, 00:13:48, Ethernet1/2
R1#
```

Figura 12. Verificación show ip route | include O/B on R1

Issue show ipv6 route command on R1; should appear as below. Verify that OSPFv3 for IPv6 is working properly.

Router R1:

```
R1#show ipv6 route
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, HA - Home Agent, MH - Mobile Router, R - RIP
        N - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS Interarea
        IS - ISIS summary, D - EIGRP, EX - EIGRP external, NN - NNDP
        ND - ND Default, NDp - ND Prefix, DCE - Destination, ND* - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        OEL - OSPF NSSA ext 1, OEL2 - OSPF NSSA ext 2, L1SP
0:::/0 [110/1], tag 0
  via FE80::113, Ethernet1/1
0::1:0:0:100:100::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:101::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:102::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:103::/64 [110/1]
  via Ethernet1/1, directly connected
R1#
```

Figura 13. Verificación show ipv6 route command on R1

Issue show ip route ospf | begin Gateway command on R3; output should appear as below. Verify that OSPF for IPv4 is working properly.

Router R3:

```
R3#show ip route ospf | begin Gateway
Gateway of last resort is 10.17.13.1 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 10.17.13.1, 00:16:06, Ethernet1/1
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O    10.17.10.0/24 [110/20] via 10.17.13.1, 00:16:06, Ethernet1/1
O    10.17.100.0/24 [110/11] via 10.17.11.2, 00:15:21, Ethernet1/0
O    10.17.101.0/24 [110/11] via 10.17.11.2, 00:15:21, Ethernet1/0
O    10.17.102.0/24 [110/11] via 10.17.11.2, 00:15:21, Ethernet1/0
R3#
```

Figura 14. Verificación de show ip route ospf | begin Gateway

Issue the show ipv6 route ospf command on R3; output should appear as below. Verify that OSPFv3 for IPv6 is working properly.

Router R3:

```
R3#show ipv6 route ospf
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, HA - Home Agent, MH - Mobile Router, R - RIP
        N - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS Interarea
        IS - ISIS summary, D - EIGRP, EX - EIGRP external, NN - NNDP
        ND - ND Default, NDp - ND Prefix, DCE - Destination, ND* - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        OEL - OSPF NSSA ext 1, OEL2 - OSPF NSSA ext 2, L1SP
0E2 ::/0 [110/1], tag 0
  via FE80::113, Ethernet1/1
0::1:0:0:100:100::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:101::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:102::/64 [110/1]
  via FE80::D11, Ethernet1/0
0::1:0:0:100:103::/64 [110/1]
  via Ethernet1/1, directly connected
R3#
```

Figura 15. Verificación show ipv6 route ospf command on R3

Verificación de la tabla de ruta IPv4

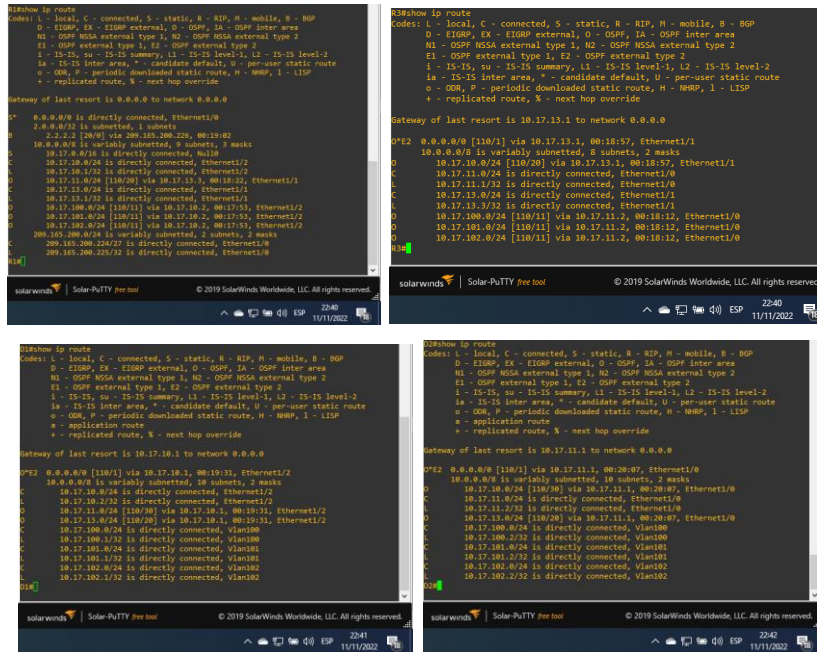


Figura 16. Verificación de la tabla de ruta IPv4

Paso 5: Verificación del MP-BGP con Ping

Ping D1 y D2 hacia Loopback 0

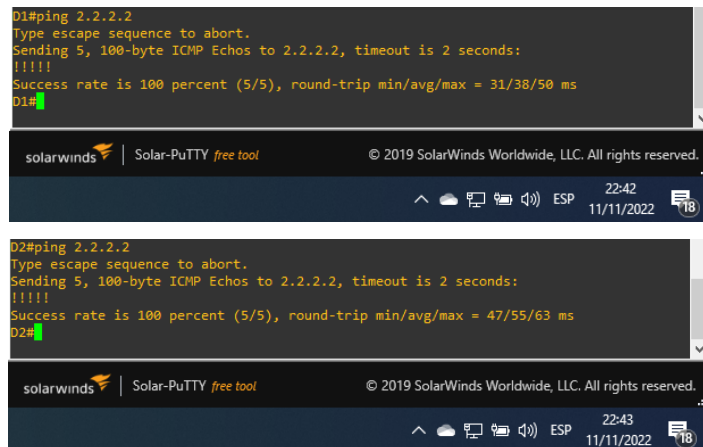


Figura 17. Verificación de Ping D1 y D2 hacia Loopback 0

PART 4 CONFIGURE FIRST HOP REDUNDANCY

Paso 1: En D1, Cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0

Switch D1:

```
ip sla 4
icmp-echo 10.17.10.1 source-ip 10.17.10.2
frequency 5
exit
ip sla schedule 4 start-time now life forever
track 4 ip sla 4 reachability
delay up 10 down 15
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
ip sla schedule 6 start-time now life forever
track 6 ip sla 6 reachability
delay up 10 down 15
exit
```

Paso 2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.

Switch D2:

```
ip sla 4
icmp-echo 10.17.11.1 source-interface e1/0
frequency 5
exit
```

```
ip sla schedule 4 start-time now life forever
track 4 ip sla 4 reachability
delay up 10 down 15
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 6 start-time now life forever
track 6 ip sla 6 reachability
delay up 10 down 15
exit
```

Paso 3: En D1 configure HSRPv2.

Switch D1:

```
interface vlan 100
standby version 2
standby 104 ip 10.17.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.17.101.254
standby 114 preempt
```



```
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.17.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Paso 4: En D2 configure HSRPv2.

Switch D2:

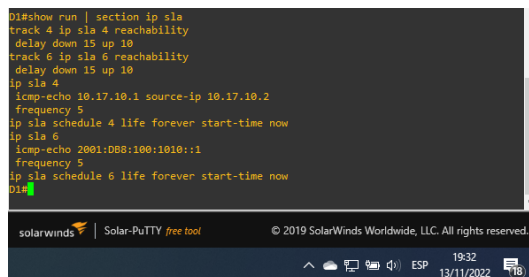
```
interface vlan 100
standby version 2
standby 104 ip 10.17.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
```

```
standby 114 ip 10.17.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.17.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

EVIDENCIAS DE CONFIGURACION PARTE 4

Issue the show run | section ip sla command on D1; output should appear as below. Verify task 4.1 and bullet 3 of task 4.3 for Switch D1.

Switch D1:



```
D1#show run | section ip sla
track 4 ip sla 4 reachability
  delay down 15 up 10
track 6 ip sla 6 reachability
  delay down 15 up 10
ip sla 4
  icmp-echo 10.17.10.1 source-ip 10.17.10.2
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Figura 18. Verificación de show run | section ip sla

Issue the show standby brief command on D1; output should appear as below. Verify task 4.3.

Switch D1:

```
D1#show standby brief
P indicates configured to preempt.

```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
V1100	104	150	P	Active	local	10.17.100.2	10.17.100.254
V1100	106	150	P	Active	local	FE80::D2:2	FE80::5:73FF:FEA0:6A
V1101	114	100	P	Standby	10.17.101.2	local	10.17.101.254
V1101	116	100	P	Standby	FE80::D2:3	local	FE80::5:73FF:FEA0:74
V1102	124	150	P	Active	local	10.17.102.2	10.17.102.254
V1102	126	150	P	Active	local	FE80::D2:4	FE80::5:73FF:FEA0:7E

Switch D2:

```
D2#show standby brief
P indicates configured to preempt.

```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
V1100	104	100	P	Standby	10.17.100.1	local	10.17.100.254
V1100	106	100	P	Standby	FE80::D1:2	local	FE80::5:73FF:FEA0:6A
V1101	114	150	P	Active	local	10.17.101.1	10.17.101.254
V1101	116	150	P	Active	local	FE80::D1:3	FE80::5:73FF:FEA0:74
V1102	124	100	P	Standby	10.17.102.1	local	10.17.102.254
V1102	126	100	P	Standby	FE80::D1:4	local	FE80::5:73FF:FEA0:7E

Figura 19. Verificación de show standby brief command on D1 y D2

Issue the show run | section ip sla command on D2; output should appear as below. Verify task 4.2 and bullet 3 of task 4.3 for Switch D2.

Switch D1:

```
D1#show run | section ip sla
track 4 ip sla 4 reachability
delay down 15 up 10
track 6 ip sla 6 reachability
delay down 15 up 10
ip sla 4
icmp-echo 10.17.10.1 source-ip 10.17.10.2
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1010::1
frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Switch D2:

```
D2#show run | section ip sla
track 4 ip sla 4 reachability
delay down 15 up 10
track 6 ip sla 6 reachability
delay down 15 up 10
ip sla 4
icmp-echo 10.17.11.1 source-Interface Ethernet1/0
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1011::1
frequency 5
ip sla schedule 6 life forever start-time now
D2#
*Nov 14 00:32:57.330: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (1), with Ethernet1/1 (999).
D2#
```

Figura 20. Verificación de show run | section ip sla command on D1 -D2

Verificación del Standby
Switch D1:

```
Switch# show run | section standby
standby version 2
standby 104 ip 10.17.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
standby version 2
standby 114 ip 10.17.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
standby version 2
standby 124 ip 10.17.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
Switch#
```

Switch D2:

```
Switch# show run | section standby
standby version 2
standby 104 ip 10.17.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 track 6 decrement 60
standby version 2
standby 114 ip 10.17.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
standby version 2
standby 124 ip 10.17.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
Switch#
```

Figura 21. Verificación de Verificación del Standby

Enlace de Handle:

CONCLUSIONES

Se puede evidenciar que los protocolos de enrutamiento utilizados en el escenario OSPF y BGP son los más comunes que se pueden encontrar en un entorno real, muchas organizaciones utilizan el OSPF para enrutar como protocolo interno porque permite que se conozca toda la red a través de la tabla de enrutamiento de cada router evitando loops, también actualizan automáticamente las tables con cualquier cambio en la topología.

El BGP para interconectar sistemas autónomos porque es normal que no todas las organizaciones utilicen el mismo protocolo de enrutamiento interno como lo es el ISP adicional sobre la importancia de las redundancias a nivel de capa 3, esta se utilizan para evitar que los dispositivos locales queden fuera de red por algún fallo en el Gateway, utilizando SLAs para monitorear continuamente las interfaces del Gateway y el protocolo HSRP para tener un router activo con la interfaz virtual y el otro de reserva.

Se puede notar como se utiliza la combinación de técnicas y protocolos Como: Redundancia de enlaces, Spanning tree y LACP para sacar el mejor provecho a la conexión en capa 2; donde el primero permite dar tolerancia a las fallas y protección contra la inoperatividad, el segundo asegura que solo exista una ruta lógica y evita bucles en estas redundancias, finalmente el LACP combina las redundancias físicas en un solo enlace lógico de alta velocidad; una combinación poderosa que se debe realizar con cuidado y en orden para no crear errores premeditados en la red.

BIBLIOGRAFÍA

BITACORDABYTE. (18 de Julio de 2017). Configurar DHCP en router CISCO. Obtenido de <https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/>

CISCO. (26 de Octubre de 2005). How to Configure SNMP Community Strings. Obtenido de <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html>

CISCO. (11 de Junio de 2020). RSTP: Configuración. Obtenido de <https://ccnadesdecero.com/curso/rstp-configuracion/>

Eugenio, G. (24 de Agosto de 2020). Como configurar IP SLA tracking. Obtenido de <https://estudiaredes.com/cisco/como-configurar-ip-sla-tracking/>

Fernández Sánchez, A. (s.f.). ¿Cómo configurar NTP en Cisco? Obtenido de <https://network-tic.com/como-configurar-ntp-en-cisco/>

NetworkLessons. (s.f.). Multiprotocol BGP (MP-BGP) Configuration. Obtenido de <https://networklessons.com/bgp/multiprotocol-bgp-mp-bgp-configuration>

Rosales, D. (2015). AAA en Routers & Switches Cisco. Obtenido de <https://delfirosales.blogspot.com/2014/04/aaa-en-routers-switches-cisco.html>