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 eltítulo 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

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ASN: *Autonomous System Number*, se le demomina 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 practicas del curso, proyectándose como opción de grado en la carrera de ingeniería en telecomunicaciones ,se desarrollan las habilidades practicas 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 swiches, 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.

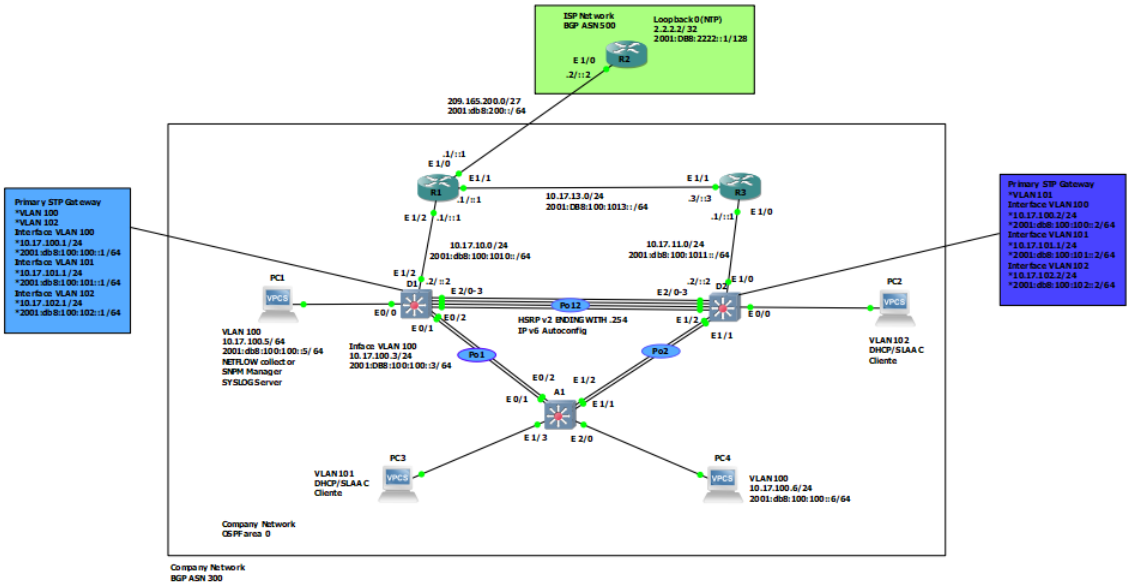


Figura 1. Montaje del escenario propuesto.

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

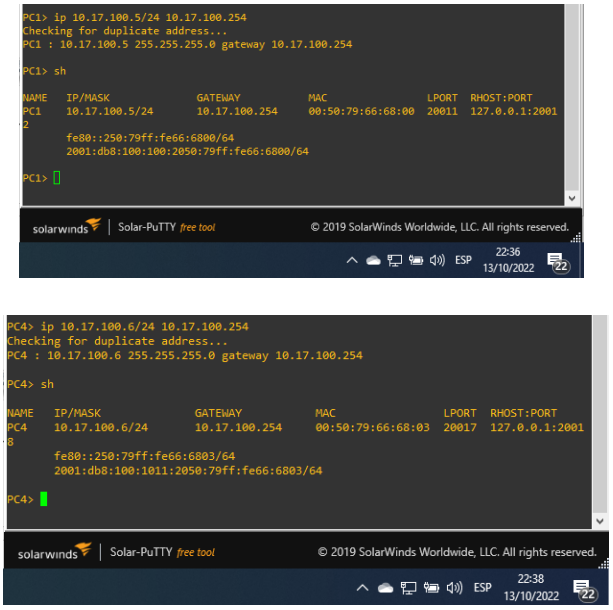


Figura 2. Configuración de IP en los PC

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

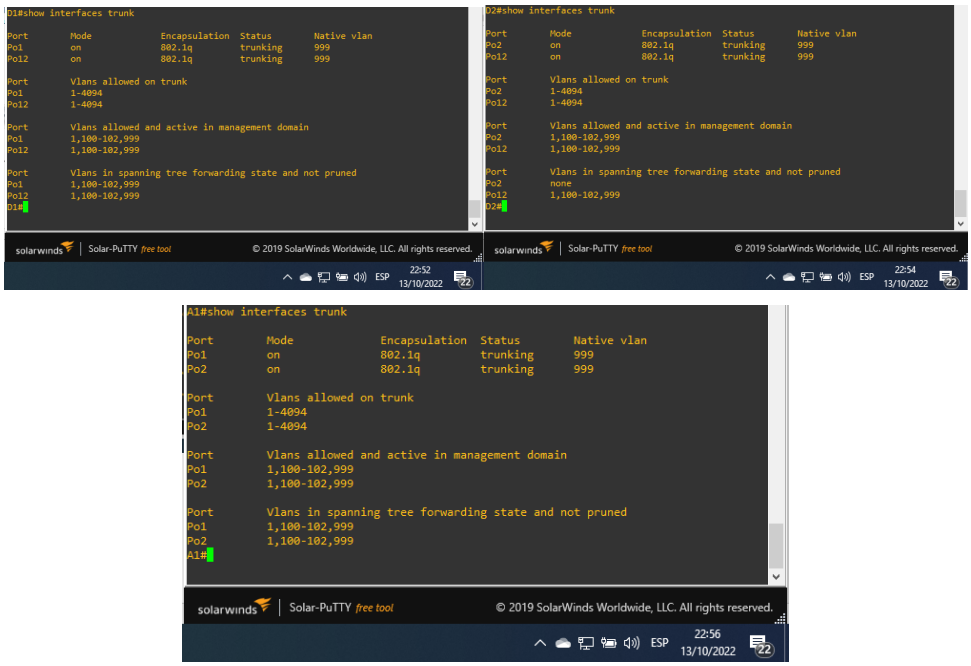


Figura 3. Verificación de los enlaces troncales

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

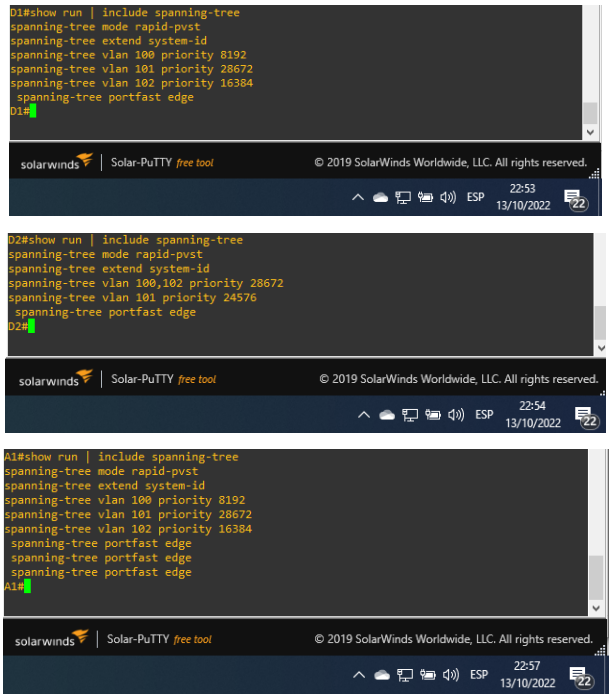


Figura 4. Verificación de spanning-tree

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

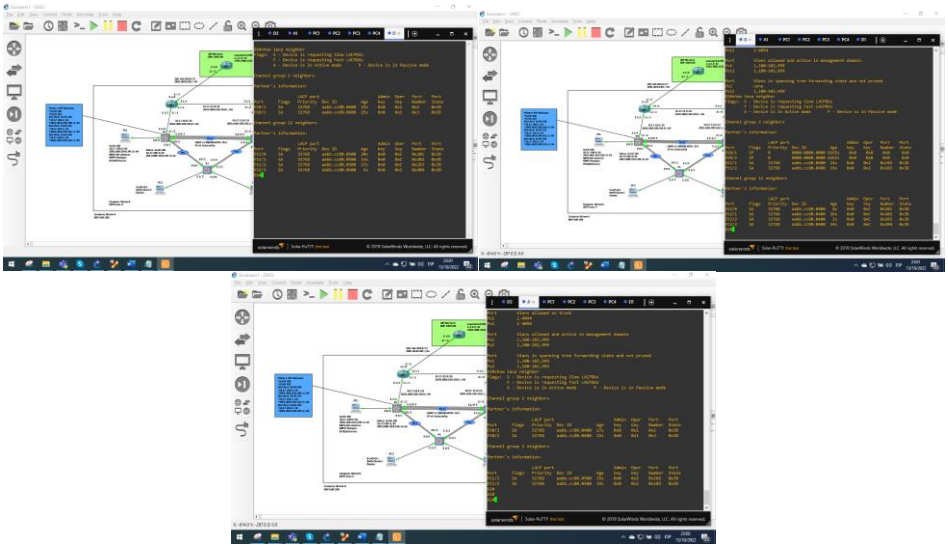


Figura 5. Verificación del LACP

Paso 7: Verificar los PC en DHCP

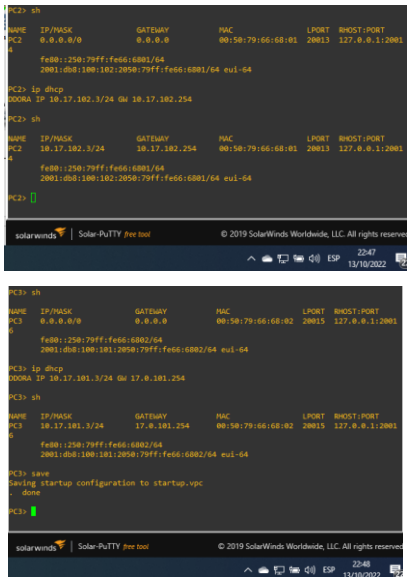


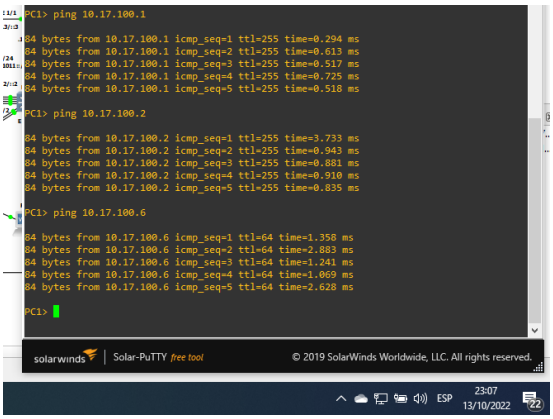
Figura 6. IP de los PC en DHCP

Paso 8: Verificación de la conectividad de la LAN local

PC1 should successfully ping:

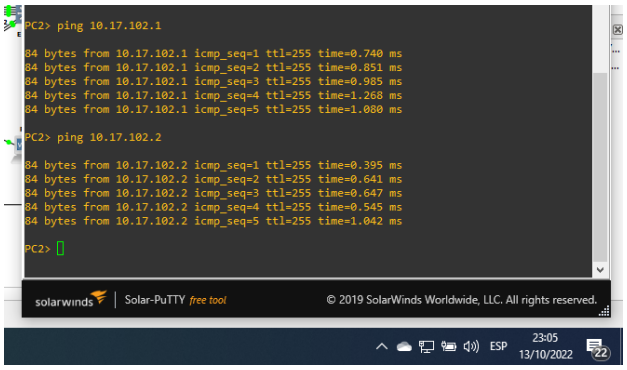
- D1: 10.53.100.1
- D2: 10.53.100.2

- PC4: 10.53.100.6



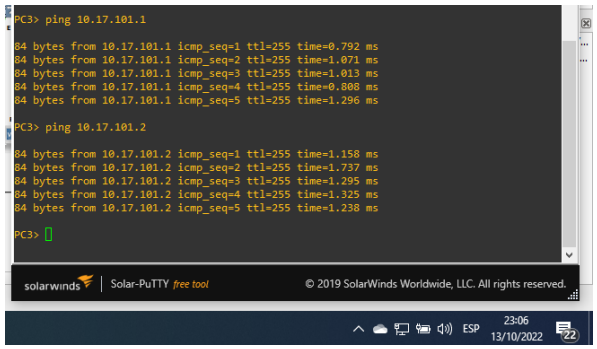
PC2 should successfully ping:

- D1: 10.53.102.1
- D2: 10.53.102.2



PC3 should successfully ping:

- D1: 10.53.101.1
- D2: 10.53.101.2



PC4 should successfully ping:

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

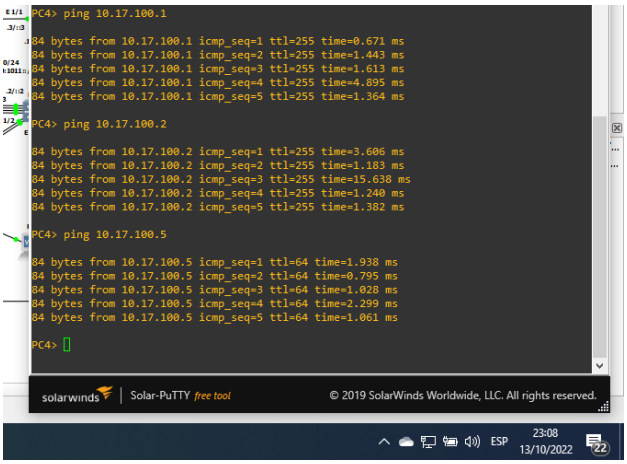


Figura 7. Ping entre los dispositivos de la red local

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

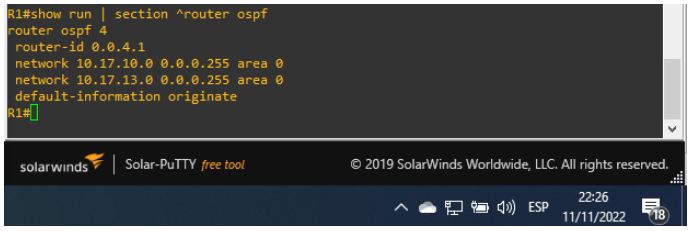
Router R1:

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

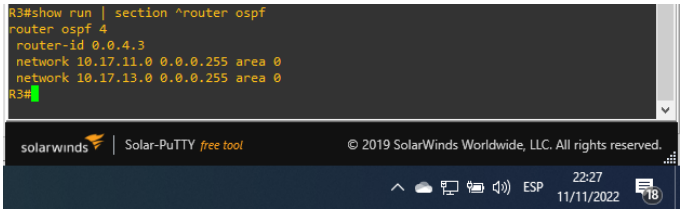
EVIDENCIAS DE CONFIGURACIÓN PARTE 3

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

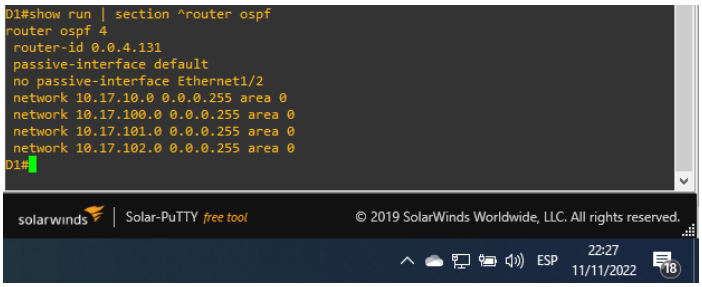
Router R1:



Router R3:



Switch D1:



Switch D2:

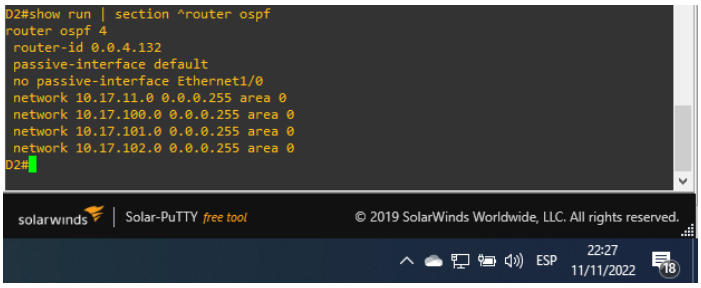
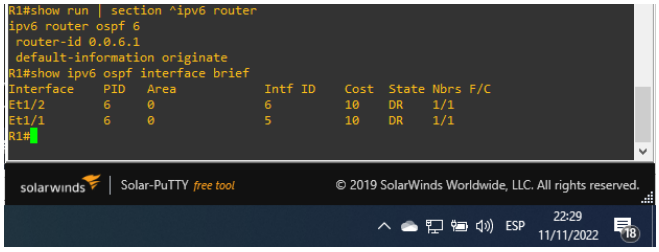


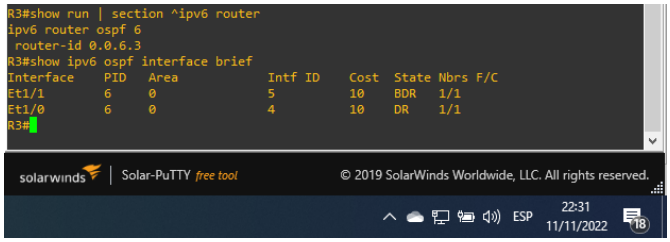
Figura 8. Verificación de show run | section ^router ospf on R1, R3, D1, and D2

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.

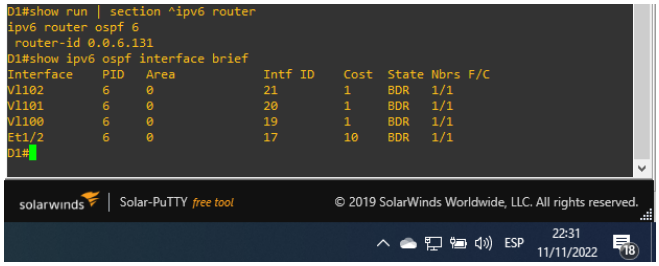
Router R1:



Router R3:



Switch D1:



Switch D2:

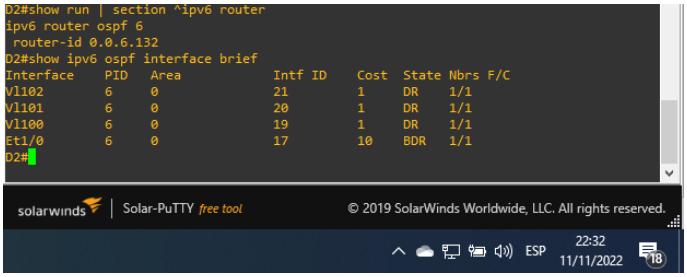


Figura 9. Verifiación show run | section ^ipv6 router and show ipv6 ospf

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

Router R2:

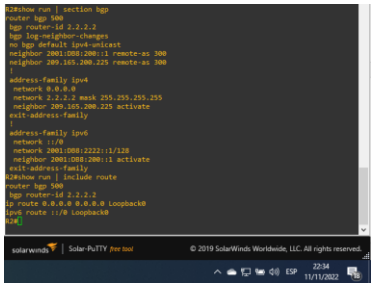


Figura 10. Verifiación show run | section bgp and show run | include route on R2

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

Router R1:

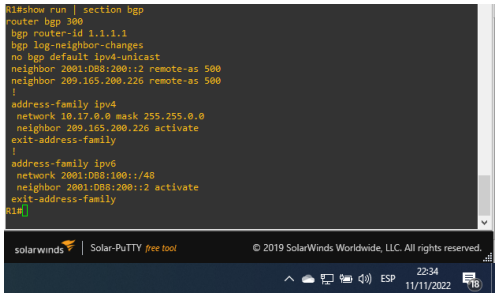


Figura 11. Verificación show run | section bgp on R1

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:

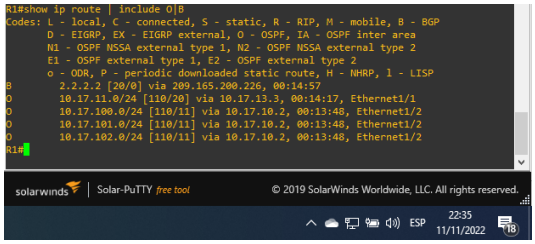


Figura 12. Verificación show ip route | include O|B on R1

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

Router R1:

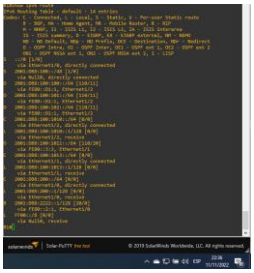


Figura 13. Verificación show ipv6 route command on R1

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:

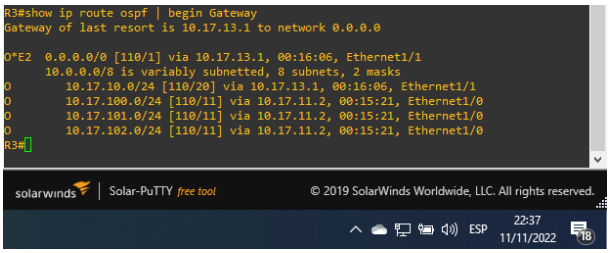


Figura 14. Verificación de show ip route ospf | begin Gateway

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

Router R3:

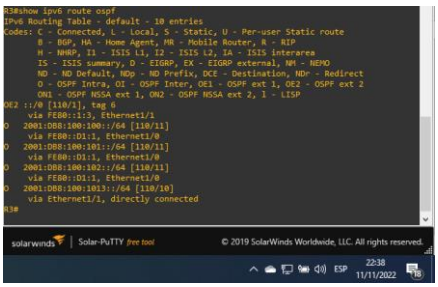


Figura 15. Verificación show ipv6 route ospf command on R3

Verificación de la tabla de ruta IPv4

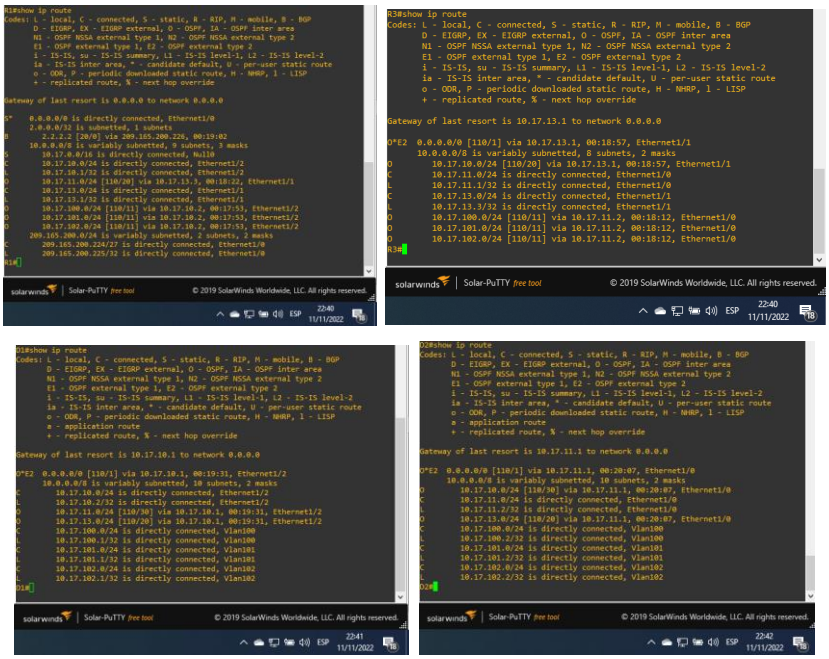


Figura 16. Verificación de la tabla de ruta IPv4

Paso 5: Verificación del MP-BGP con Ping

Ping D1 y D2 hacia Loopback 0

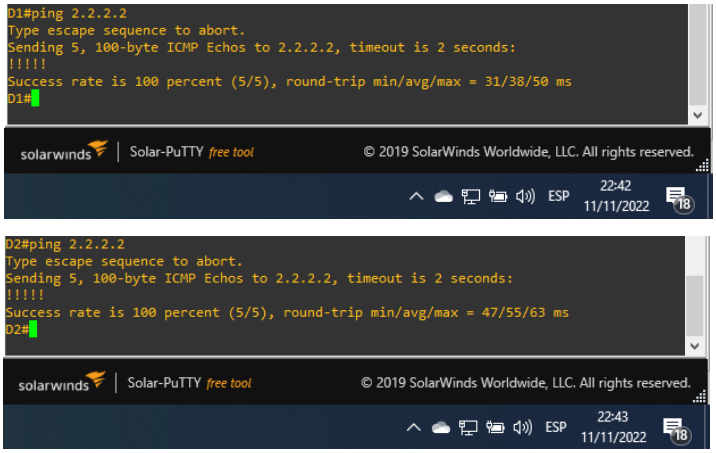


Figura 17. Verificación de Ping D1 y D2 hacia Loopback 0

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:

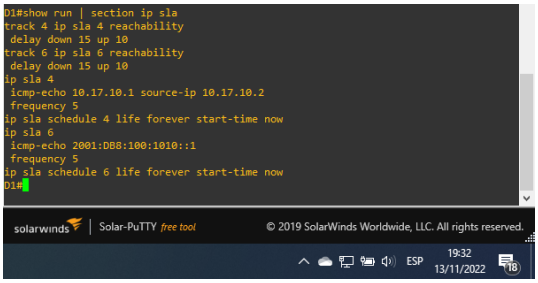
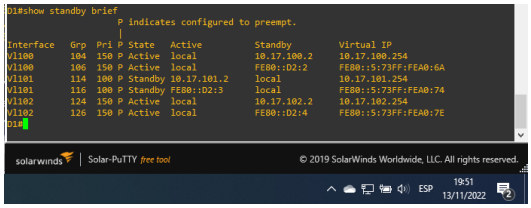


Figura 18. Verificación de show run | section ip sla

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

Switch D1:



Switch D2:

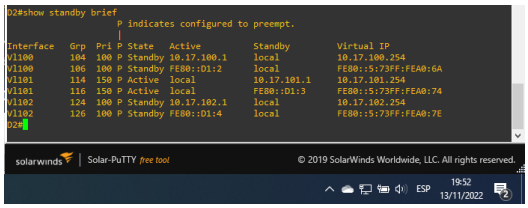
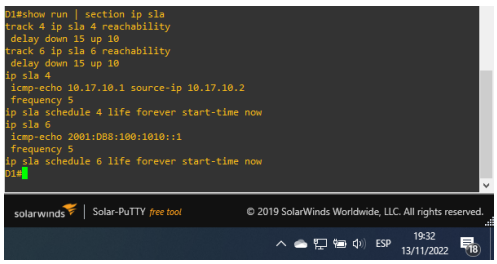


Figura 19. Verificación de show standby brief command on D1 y D2

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:



Switch D2:

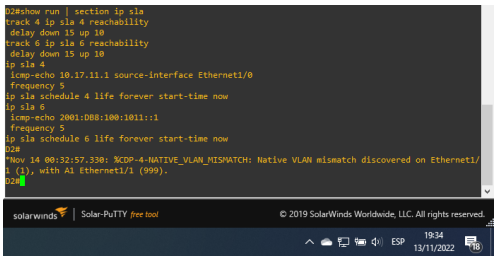


Figura 20. Verificación de show run | section ip sla command on D1 -D2

Verificación del Standby

Switch D1:

Switch D2:

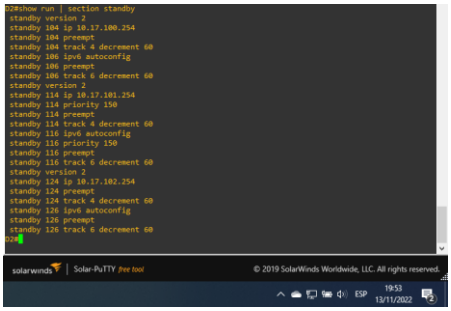


Figura 21. Verificación de Verificación del Standby

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