

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR ROBINSON PONTON

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR ROBINSON PONTON

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Yopal, 13 de noviembre del 2021

AGRADECIMIENTOS

Dedicado primeramente a Dios todo poderoso que me dio la voluntad de seguir adelante incluso cuando ni yo mismo sentía que lo podía lograr, mis padres, hermanos y tías que me dieron ánimo y me hicieron reflexionar en todo momento sobre la importancia de apasionarse por cada una de las cosas que hacemos, Elisa por confiar en mí todo momento y colaborarme en momentos que necesitaba que ayude, en estos momentos que creí que no podía, en memoria de las personas que no están acá pero su recuerdo y alma vive día tras día.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN.....	12
DESARROLLO	13
ESCENARIO 1	13
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.....	15
Parte 2: Configurar la capa 2 de la red y el soporte de Host	27
Parte 3: Configurar los protocolos de enrutamiento	40
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)	58
Parte 5: Seguridad.....	72
Parte 6: Configure las funciones de Administración de Red.....	78
CONCLUSIONES	85
BIBLIOGRAFÍA.....	86

LISTA DE TABLAS

Tabla 1	Direccionamiento Topología de RED	13
Tabla 2	Configuración de la capa 2 de la RED	27
Tabla 3	Configuración de los protocolos de enrutamiento	40
Tabla 4	Configuración de la Redundancia del Primer Salto (First Hop Redundancy)	58
Tabla 5	Configuración de Seguridad.....	72
Tabla 6	Configuración de las funciones de Administración de la RED.....	78

LISTA DE FIGURAS

Ilustración 1 Ilustración 1 Fuente: Simulador Packet Tracer 8. Captura tomada por el Autor	13
Ilustración 2 Topología de Red ISP.....	14
Ilustración 3 Configuración R1	16
Ilustración 4 Configuración R2	17
Ilustración 5 Configuración R3	18
Ilustración 6 Configuración Switch D1.....	20
Ilustración 7 Configuración D2	22
Ilustración 8 Configuración Switch A1.....	24
Ilustración 9 Copia del archivo running-config al archivo startup-config.....	25
Ilustración 10 Configuración IP PC 1	26
Ilustración 11 Configuración IP PC4	26
Ilustración 12 activación enlaces trunk 802.1Q.....	29
Ilustración 13 Configuración VLAN Nativa	30
Ilustración 14 Activación protocolo Rapid Spanning-Tree (RSTP).....	31
Ilustración 15 Configuración puentes raíz RSTP.....	32
Ilustración 16 EtherChannels LACP.....	32
Ilustración 17 activación channel-group 2 mode active.....	33
Ilustración 18 Activación channel-group 1 mode.....	33
Ilustración 19 Configuración de los puertos de acceso del host.....	34
Ilustración 20 Verificación servicios DHCP IPv4 PC2	34
Ilustración 21 Verificación servicios DHCP IPv4 PC3	35
Ilustración 22 Ping PC1 a D1	35
Ilustración 23 Ping PC1 a D2.....	36
Ilustración 24 Ping PC1 al PC4.....	36
Ilustración 25 Ping PC2 a D1	37
Ilustración 26 Ping PC1 a D2.....	37
Ilustración 27 Ping de PC 3 a D1 y D2.....	38
Ilustración 28 Ping de PC 4 a D1	38
Ilustración 29 Ping de PC 4 a D2	39
Ilustración 30 Ping del PC4 al PC1	39
Ilustración 31 Configuración OSPFv2 en area 0 de R1.....	43
Ilustración 32 Configuración OSPFv2 en area 0 de R3.....	44
Ilustración 33 Configuración OSPFv2 en area 0 de D1.....	46
Ilustración 34 Configuración OSPFv2 en area 0 de D2.....	48
Ilustración 35 Configuración OSPFv3 en R1.....	49
Ilustración 36 Configuración OSPFv3 en R3.....	50
Ilustración 37 Configuración OSPFv3 en D1.....	51
Ilustración 38 Configuración OSPFv3 en D2.....	52

Ilustración 39 verificación configuración BGP mediante el comando (Show ip BGP neighbor) en R3	55
Ilustración 40 verificación configuración BGP mediante el comando (Show ip BGP neighbor) en R1	57
Ilustración 41 Comando SLAs no soportado por packet Tracer.....	61
Ilustración 42 Comando SLAs no soportado por packet Tracer en D2	63
Ilustración 43 Verificación standby en D1	68
Ilustración 44 Verificación standby en D2	71
Ilustración 45 Validación de la configuración Server RADIUS	77
Ilustración 46 Configuración hora en R1	79
Ilustración 47 Verificación NTP en R1.....	82

GLOSARIO

DHCP: es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Red ISP: El proveedor de servicios de internet (ISP, por las siglas de Internet Service Provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como ADSL, cable módem, GSM, dial-up, etc.

Packet Tracer: es una aplicación a través de la cual se puede realizar una gran variedad de funciones relacionadas con las redes, como diseñar y construir una red desde cero, trabajar sobre proyectos pre construidos (incluye una gran variedad de ejemplos interesantes), probar nuevos diseños y topologías de red, probar cambios en la red antes de aplicarlos a la misma, examinar el flujo de datos a través de una red.

SLAAC: es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP.

INTERFACES TRONCALES DE LAS VLAN: Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

HSRP: Es la posibilidad de asignar direcciones IP virtuales a cada grupo. Si el router primario deja de funcionar, el secundario ocupará su lugar, mientras que la dirección IP virtual seguirá siendo la misma.

Router: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Switch: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN).

RESUMEN

Diplomado de Profundización CCNP, busca identificar el grado de desarrollo de competencias y habilidades que se adquieren a lo largo del diplomado para Profesionales en las áreas de desarrollo de sistemas, telecomunicaciones, electrónica y carreras afines, con conocimiento básico en redes, que trabajen brindando soporte o administrando redes de comunicación de datos.

El documento expresa las características fundamentales en el diseño y resolución de problemas en una red de telecomunicaciones bajo estándares Cisco. Los fundamentos de Conmutación, Enrutamiento e Inalámbricos se enfoca en tecnologías de conmutación y operaciones de enrutadores que admiten de pequeñas a medianas redes empresariales; lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking. En esta prueba de habilidades, se debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la Red en la topología.

Para esta actividad, se debe realizar las tareas asignadas en el escenario propuesto, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante el desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route.

Palabras Clave: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

ABSTRACT

CCNP Deepening Diploma, seeks to identify the degree of development of competencies and skills that are acquired throughout the diploma for Professionals in the areas of systems development, telecommunications, electronics and related careers, with basic knowledge in networks, who work providing support or managing data communication networks.

The document expresses the fundamental characteristics in the design and resolution of problems in a telecommunications network under Cisco standards. The Fundamentals of Switching, Routing and Wireless focuses on switching technologies and router operations that support small to medium business networks; The essential thing is to test the levels of understanding and problem solving related to various aspects of Networking. In this skills test, the network configuration must be completed for complete end-to-end accessibility, for hosts to have reliable support of the default gateway, and for configured protocols to be operational within the Network portion of the topology.

For this activity, the tasks assigned in the proposed scenario must be carried out, accompanied by the respective documentation processes of the solution, corresponding to the registration of the configuration of each of the devices, the detailed description of the step by step of each of the devices. The stages carried out during development, the registration of the connectivity verification processes by using the commands ping, traceroute, show ip route.

Keywords: CISCO, CCNP, ROUTING, SWITCHING, NETWORKING,
ELECTRONICS

INTRODUCCIÓN

En el presente documento se puede encontrar el desarrollo de dos escenarios que pueden impartirse en un ambiente real, donde se presentan unas características relacionadas a la personalización del funcionamiento de una red de telecomunicaciones Cisco.

Se busca construir una red ISP y configurar los ajustes básicos de cada uno de los dispositivos y el direccionamiento de las interfaces para un fin determinado por una compañía, donde se generaliza los protocolos de enrutamiento como BGP, configuración de puertos en switches con sus datos de red y vlan. Mediante los comandos (show / ping) se verificaran las conexiones y su correcta sincronización. Con esto se obtiene las habilidades necesarias para poder trabajar en sistemas de red, seguridad, enlaces, configuraciones de direcciones IP, generación de canales y enlaces para que los routers logren una conexión adecuada y una seguridad apropiada para no poner en riesgo el tráfico de datos entre los puntos de la red.

Se busca que como estudiantes encuentren soluciones a un determinado proceso donde implica el uso de muchos elementos como equipos router, switches, cableado, enlaces, protocolos y direccionamiento para enfocar la red a las necesidades del usuario, mediante el software usado en cisco packet tracer donde se validan las diferentes configuraciones. Se realiza ilustraciones del paso a paso donde se pueden evidenciar las diferentes configuraciones y enlaces de red, funcionalidades y demás aspectos importantes sobre enrutamiento y conectividad.

DESARROLLO

ESCENARIO 1

Topología de la Red:

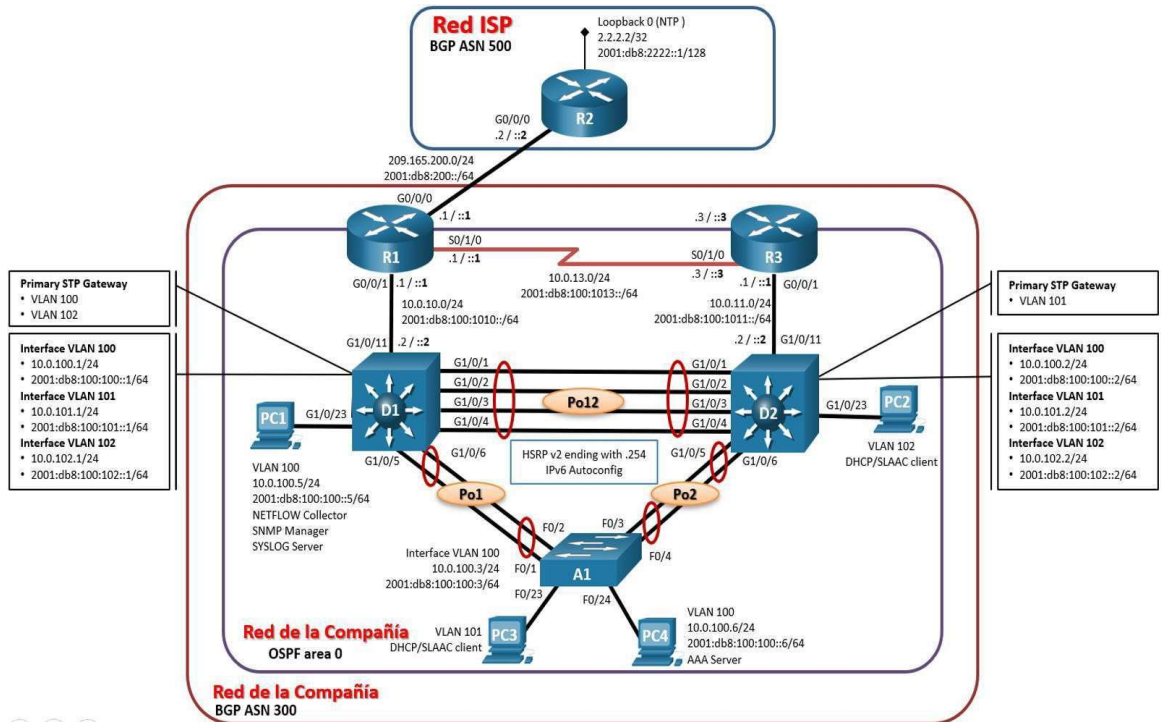


Ilustración 1 Ilustración 1 Fuente: Simulador Packet Tracer 8. Captura tomada por el Autor

Tabla 1 Direccionamiento Topología de RED

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
R1	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
R1	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
R2	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
R3	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
D1	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
D1	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
D1	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
D2	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
D2	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
D2	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

Montaje de la Topología propuesta mediante el aplicativo Packet Tracer

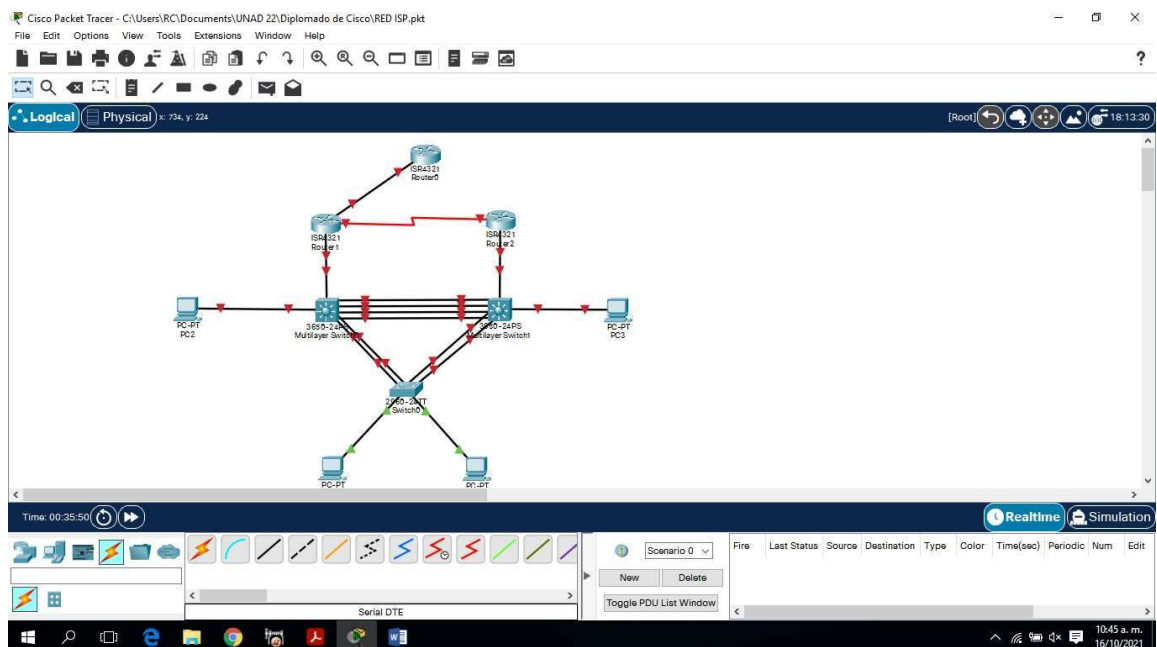


Ilustración 2 Topología de Red ISP

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Paso 1: Cablear la red como se muestra en la topología.

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

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:

Router R1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config) #hostname R1
R1(config)#ipv6 unicast-routing
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 g0/0/0
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 g0/0/1
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)#exit
R1(config)#interface s0/1/0
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
```

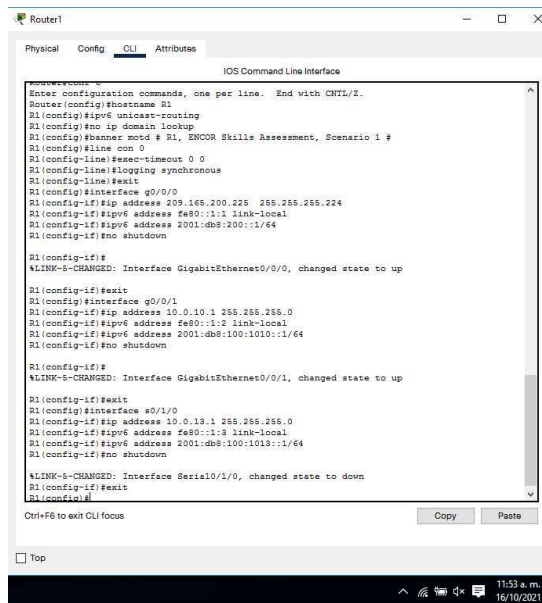


Ilustración 3 Configuración R1

Router R2

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(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 g0/0/0

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

R2(config)#interface Loopback 0

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

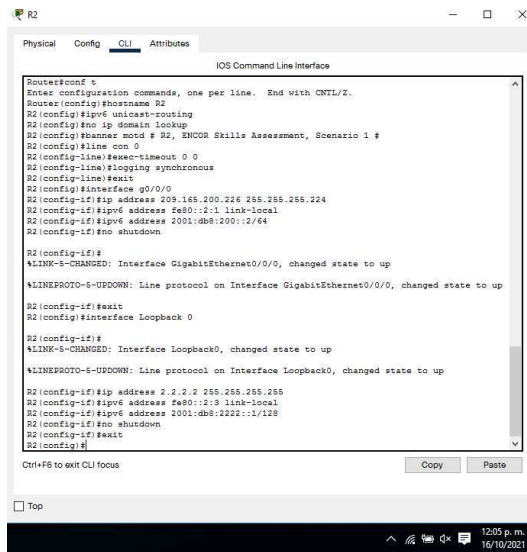


Ilustración 4 Configuración R2

Router R3

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(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 g0/0/1

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

R3(config)#interface s0/1/0

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

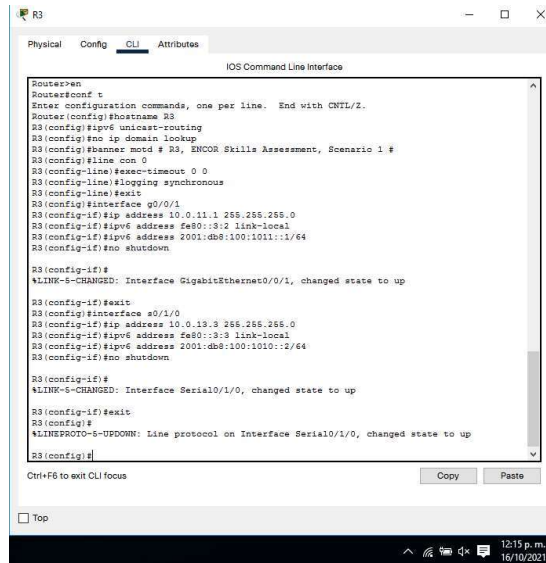


Ilustración 5 Configuración R3

Switch D1

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname D1
D1(config)#ip routing
D1(config)#ip v6 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 g1/0/11

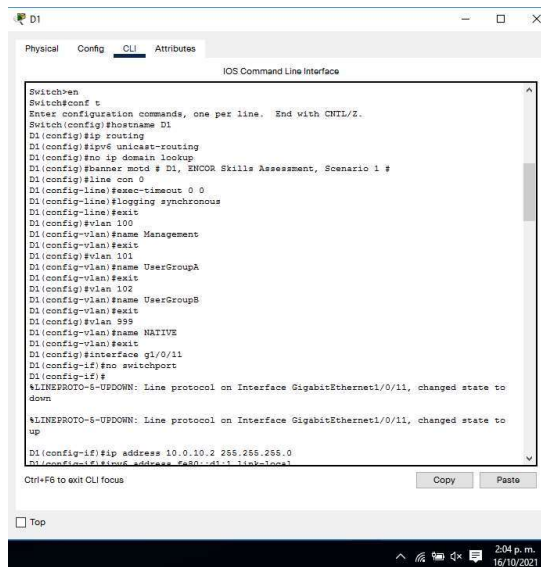
```

```

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)#
%LINK-5-CHANGED: Interface Vlan102, changed state to up
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)#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 g1/0/1-10
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#interface range g1/0/12-24
D1(config-if-range)#shutdown
D1(config-if-range)#exit

```

```
D1(config)#interface range g1/1/1-4
D1(config-if-range)#shutdown
```



```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 g1/0/11
D1(config-if)#no switchport
D1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11, changed state to
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11, changed state to
up
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#end
Switch#
```

Ilustración 6 Configuración Switch D1

Switch D2

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 g1/0/11
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::d2:4 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 g1/0/1-10
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range g1/0/12-24
D2(config-if-range)#shutdown
D2(config-if-range)#exit

```

```
D2(config)#interface range g1/1/1-4
D2(config-if-range)#shutdown
D2(config-if-range)#exit
```

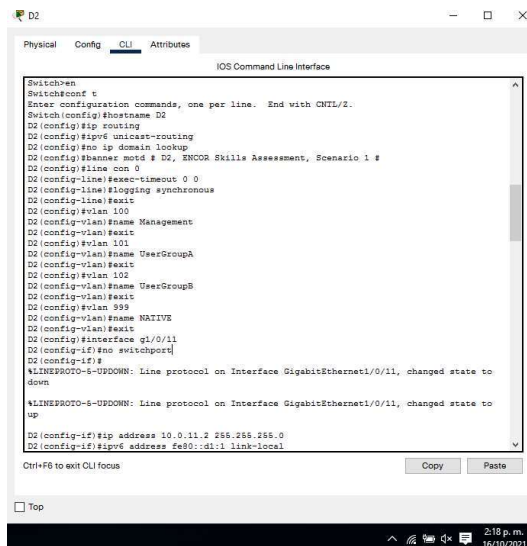


Ilustración 7 Configuración D2

Switch A1

```
A1>en
A1#conf t
A1(config)#sdm prefer dual-ipv4-and-ipv6 default
A1(config)# exit
A1#
%SYS-5-CONFIG_: Configured from console by console
A1#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
memory.
2960-24TT starting...
Base ethernet MAC Address: 000B.BE8A.E530
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 3 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
```

```
flashfs[0]: Bytes used: 4672499
flashfs[0]: Bytes available: 59343885
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
```

```
Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
```

```
#####
```

```
##### [OK]
```

```
Smart Init is enabled
```

```
smart init is sizing iomem
```

```
TYPE MEMORY_REQ
```

```
TOTAL: 0x00000000
```

```
Rounded IOMEM up to: 0Mb.
```

```
Using 6 percent iomem. [0Mb/512Mb]
```

```
A1>en
```

```
A1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
A1(config)#hostname A1
```

```
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 f0/5-22
```

```

A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
A1#

```

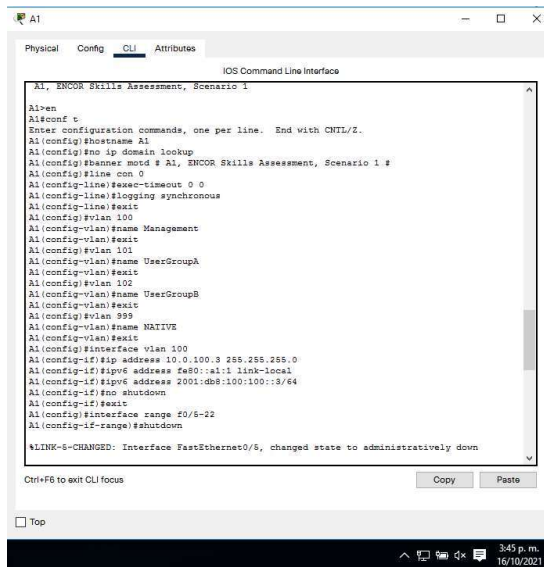
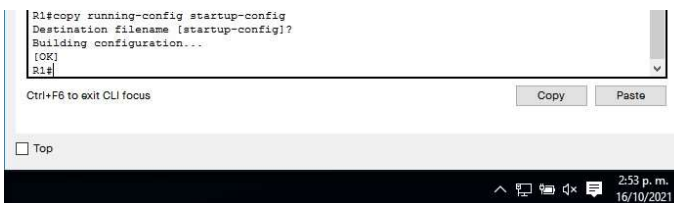
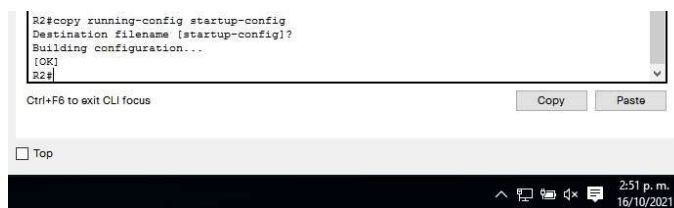


Ilustración 8 Configuración Switch A1

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



```
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

2:54 p. m.
16/10/2021

```
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
D1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

2:48 p. m.
16/10/2021

```
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
D2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

2:50 p. m.
16/10/2021

```
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
A1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

3:45 p. m.
16/10/2021

Ilustración 9 Copia del archivo running-config al archivo startup-config

- c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

PC 1

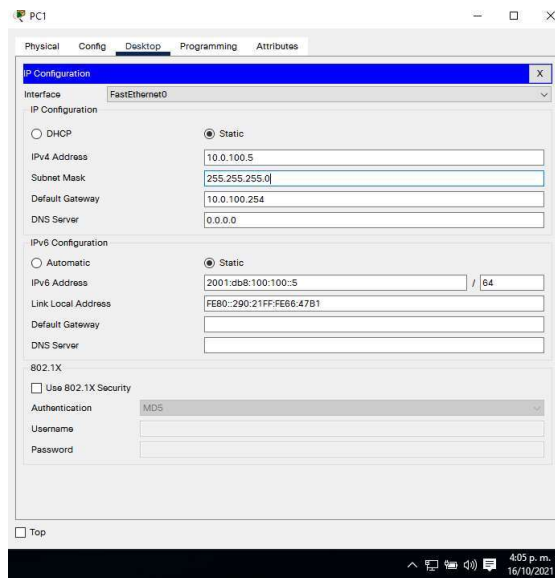


Ilustración 10 Configuración IP PC 1

PC4

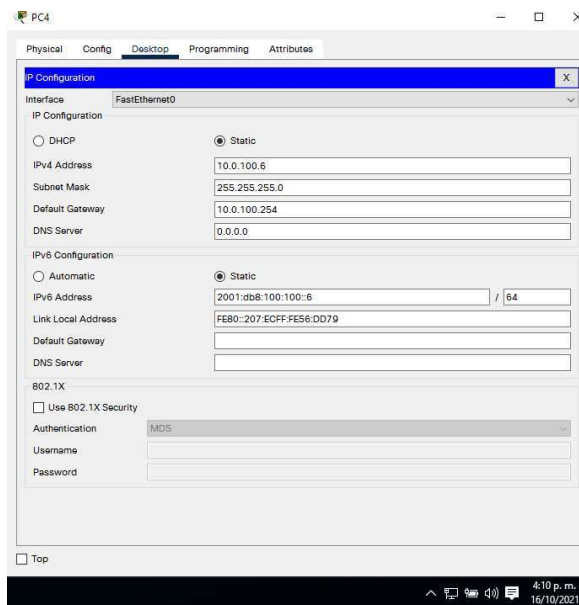


Ilustración 11 Configuración IP PC4

Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Tabla 2 Configuración de la capa 2 de la RED

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	<p>PC1 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Habilite enlaces trunk 802.1Q entre:

- D1 and D2

D1>en

D1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

D1(config)#interface range g1/0/1-4

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

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

D1(config-if-range)#interface range g1/0/5-6

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

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

D1(config-if-range)#

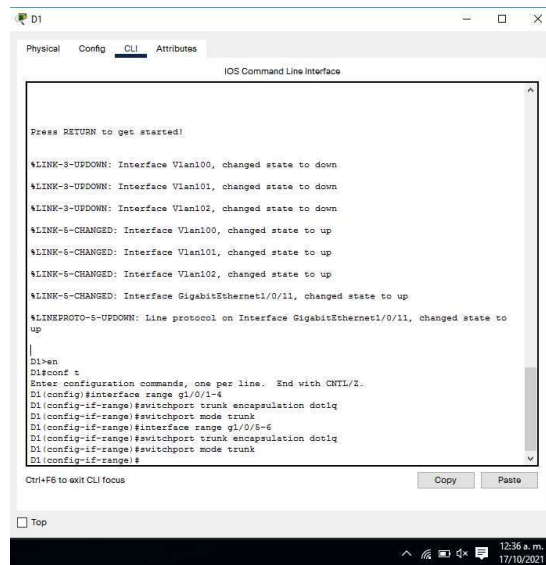


Ilustración 12 activación enlaces trunk 802.1Q

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

Use VLAN 999 como la VLAN nativa.

```

D1>en
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#interface range g1/0/1-4
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 12
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
Configuración de un enlace troncal 802.1Q

```

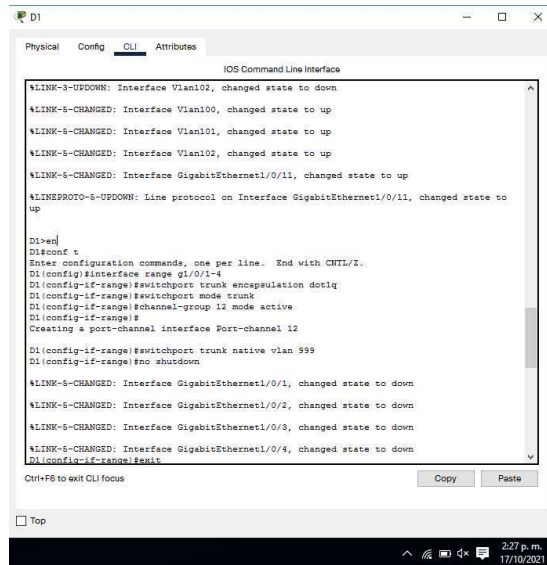


Ilustración 13 Configuración VLAN Nativa

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

Use Rapid Spanning Tree (RSPT).

```

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 g1/0/23
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 GigabitEthernet1/0/23 but will only
have effect when the interface is in a non-trunking mode.
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#end

```

```

D1
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 g1/0/23
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 GigabitEthernet1/0/23 but will only
have effect when the interface is in a non-trunking mode.
D1 (config-if)#no shutdown

D1 (config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

D1 (config-if)#exit
D1 (config)#end
D1#
%SYS-6-CONFIG_I: Configured from console by console
D1#

```

Ilustración 14 Activación protocolo Rapid Spanning-Tree (RSTP)

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

```

D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface g1/0/23
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100

```

```

D1
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to down
%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po1 and will be suspended (native
vian of Gig1/0/6 is 999, Po1 id 1)
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 g1/0/23
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 GigabitEthernet1/0/23 but will only
have effect when the interface is in a non-trunking mode.
D1(config-if)#no shutdown
D1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
D1(config-if-range)#exit
D1(config)#end
D1#
Ctrl+F8 to exit CLI focus
Copy Paste
Top
5:38 p.m.
17/10/2021

```

Ilustración 15 Configuración puentes raíz RSTP

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

Use los siguientes números de canales:

- • D1 a D2 – Port channel 12
- • D1 a A1 – Port channel 1
- • D2 a A1 – Port channel 2

D1(config-if-range)#channel-group 12 mode active

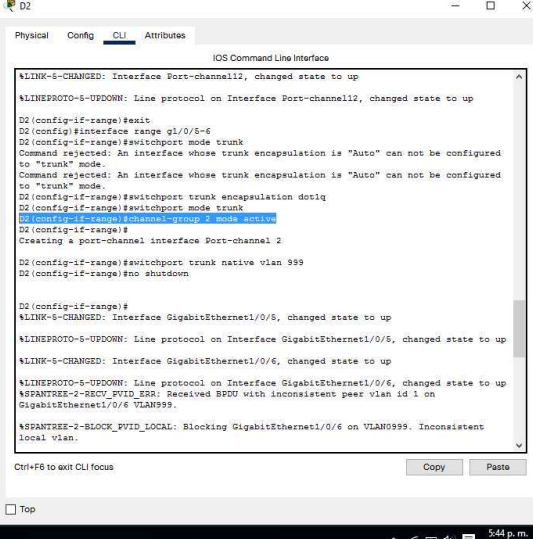
```

D1
Physical Config CLI Attributes
IOS Command Line Interface
D1(config)#
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#interface range g1/0/1-4
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 12
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to down
D1(config-if-range)#exit
D1(config)#interface range g1/0/5-6
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
D1(config-if-range)#
Creating a port-channel interface Port-channel 1
%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po1 and will be suspended (native
vian of Gig1/0/5 is 999, Po1 id 1)
%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po1 and will be suspended (native
vian of Gig1/0/6 is 999, Po1 id 1)
D1(config-if-range)#no shutdown
D1(config-if-range)#
Ctrl+F8 to exit CLI focus
Copy Paste
Top
5:47 p.m.
17/10/2021

```

Ilustración 16 EtherChannels LACP

D2(config-if-range)#channel-group 2 mode active



```
Physical Config CLI Attributes
IOS Command Line Interface

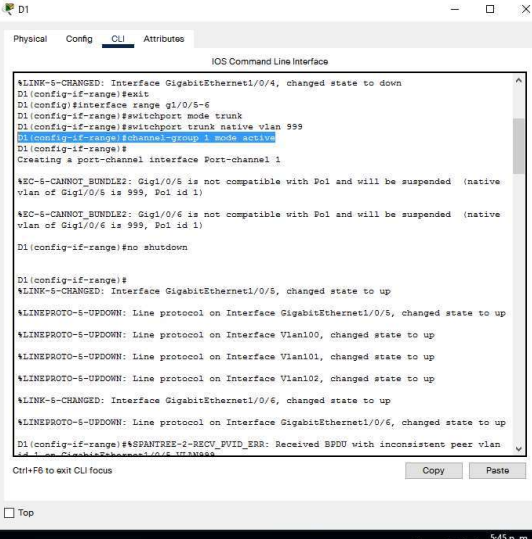
%LINK-5-CHANGED: Interface Port-channel12, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel12, changed state to up
D2(config-if-range)#exit
D2(config)#interface range g1/0/5-6
D2(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 2
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#no shutdown

D2(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on GigabitEthernet1/0/6 VLAN999.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet1/0/6 on VLAN999. Inconsistent local vlan.

Ctrl+F8 to exit CLI focus
Copy Paste
```

Ilustración 17 activación channel-group 2 mode active

D1(config-if-range)#channel-group 1 mode active



```
Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to down
D1(config-if-range)#exit
D1(config)#interface range g1/0/5-6
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
D1(config-if-range)#
Creating a port-channel interface Port-channel 1
%EC-5-CANNOT_BUNDLE2: G1g1/0/5 is not compatible with Po1 and will be suspended (native vlan of G1g1/0/5 is 999, Po1 id 1)
%EC-5-CANNOT_BUNDLE2: G1g1/0/6 is not compatible with Po1 and will be suspended (native vlan of G1g1/0/6 is 999, Po1 id 1)
D1(config-if-range)#no shutdown

D1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet1/0/6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to up
D1(config-if-range)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on GigabitEthernet1/0/6 VLAN999.

Ctrl+F8 to exit CLI focus
Copy Paste
```

Ilustración 18 Activación channel-group 1 mode

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

A1(config-if)#switchport access vlan 101

```
A1
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to up
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface f0/23
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(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 FastEthernet0/23 but will only
have effect when the interface is in a non-trunking mode.
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface f0/24
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(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 FastEthernet0/24 but will only
have effect when the interface is in a non-trunking mode.
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#end
A1#
%SYS-5-CONFIG I: Configured from console by console
Ctrl+F6 to exit CLI focus
```

Ilustración 19 Configuración de los puertos de acceso del host

2.7 Verifique los servicios DHCP IPv4.

PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>show running-config | section dhcp
Invalid Command.

C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix... :
Physical Address. . . . . : 000B.BE48.8A86
Link-local IPv6 Address. . . . . : FE80::20B:BB7F:FE48:8A86
IPv4 Address. . . . . : 10.0.102.210
Subnet Mask. . . . . : 255.255.252.0
Default Gateway. . . . . : 10.0.102.1
DHCP Server. . . . . : 10.0.102.1
DHCPv6 IAID. . . . . :
DHCPv6 Client DUID. . . . . : 00-01-00-01-00-60-8D-75-00-08-BE-48-8A-86
DNS Servers. . . . . :
0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix... :
Physical Address. . . . . : 0090.0C52.0CB9
Link-local IPv6 Address. . . . . :
--More--
```

Ilustración 20 Verificación servicios DHCP IPv4 PC2

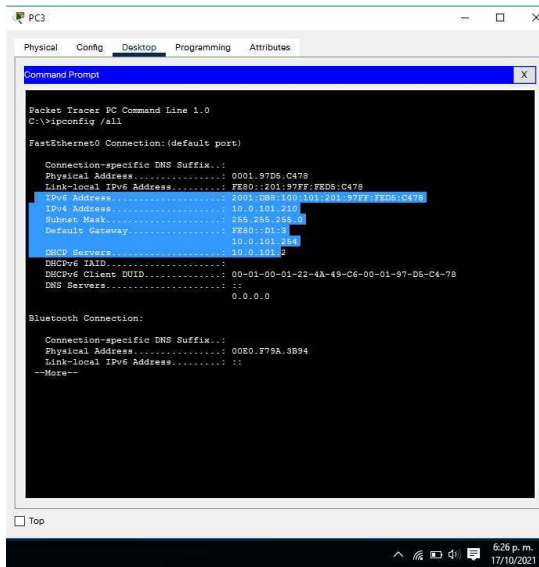


Ilustración 21 Verificación servicios DHCP IPv4 PC3

2.8 Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

- D1: 10.0.100.1

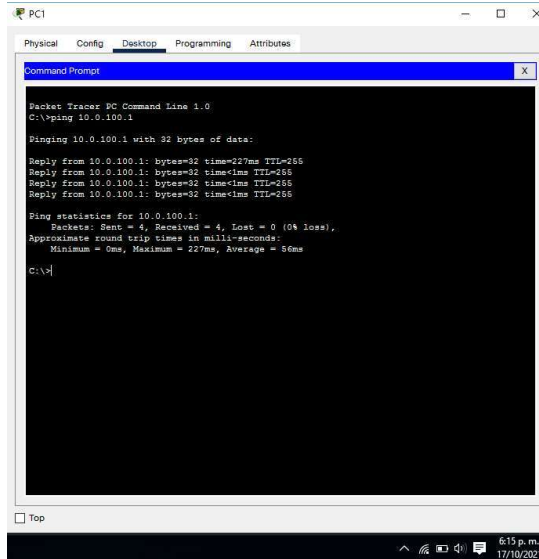


Ilustración 22 Ping PC1 a D1

- D2: 10.0.100.2

```

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.100.1

Pinging 10.0.100.1 with 32 bytes of data:

Reply from 10.0.100.1: bytes=32 time=227ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 227ms, Average = 66ms

C:\>ping 10.0.100.2

Pinging 10.0.100.2 with 32 bytes of data:

Reply from 10.0.100.2: bytes=32 time=63ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 63ms, Average = 15ms

C:\>

```

Ilustración 23 Ping PC1 a D2

- PC4: 10.0.100.6

```

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 63ms, Average = 15ms

C:\>10.0.100.6
Invalid Command.

C:\>ping 10.0.100.6

Pinging 10.0.100.6 with 32 bytes of data:

Request timed out.
Reply from 10.0.100.6: bytes=32 time=92ms TTL=128
Reply from 10.0.100.6: bytes=32 time=21ms TTL=128
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.100.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 92ms, Average = 34ms

C:\>ping 10.0.100.6

Pinging 10.0.100.6 with 32 bytes of data:

Reply from 10.0.100.6: bytes=32 time<1ms TTL=128
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128
Reply from 10.0.100.6: bytes=32 time=96ms TTL=128
Reply from 10.0.100.6: bytes=32 time=109ms TTL=128

Ping statistics for 10.0.100.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 109ms, Average = 48ms

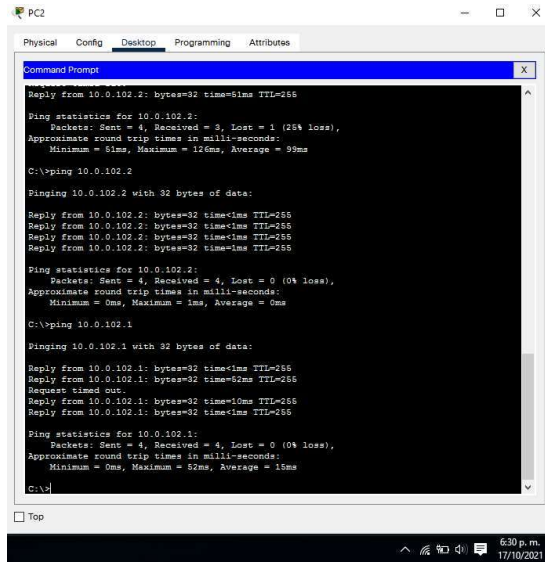
C:\>

```

Ilustración 24 Ping PC1 al PC4

PC2 debería hacer ping con éxito a:

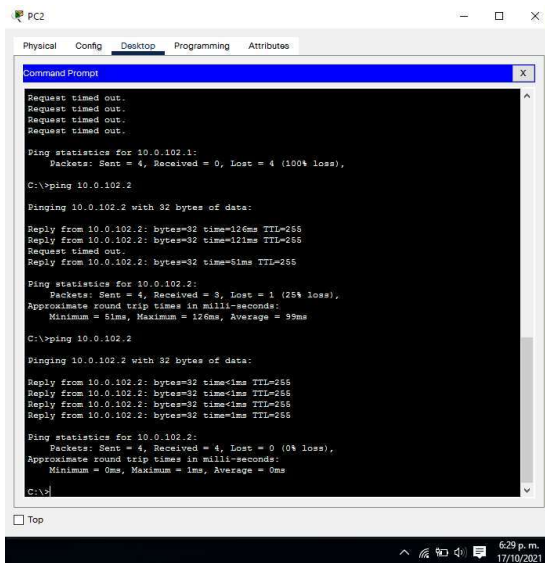
- D1: 10.0.102.1



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.0.102.2: bytes=32 time=51ms TTL=255
Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 126ms, Average = 99ms
C:\>ping 10.0.102.2
Pinging 10.0.102.2 with 32 bytes of data:
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.0.102.1
Pinging 10.0.102.1 with 32 bytes of data:
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time=52ms TTL=255
Request timed out.
Reply from 10.0.102.1: bytes=32 time=10ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.0.102.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 52ms, Average = 15ms
C:\>
```

Ilustración 25 Ping PC2 a D1

- D2: 10.0.102.2



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.102.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 10.0.102.2
Pinging 10.0.102.2 with 32 bytes of data:
Reply from 10.0.102.2: bytes=32 time=126ms TTL=255
Reply from 10.0.102.2: bytes=32 time=121ms TTL=255
Request timed out.
Reply from 10.0.102.2: bytes=32 time=51ms TTL=255
Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 51ms, Maximum = 126ms, Average = 99ms
C:\>ping 10.0.102.2
Pinging 10.0.102.2 with 32 bytes of data:
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Ilustración 26 Ping PC1 a D2

PC3 debería hacer ping con éxito a:

- D1: 10.0.101.1
- D2: 10.0.101.2

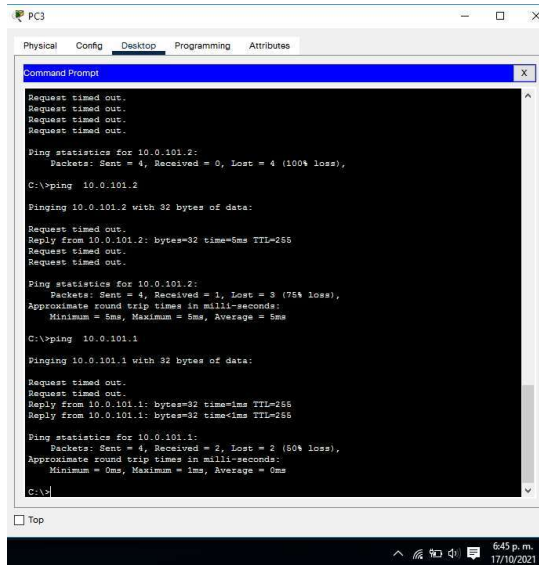


Ilustración 27 Ping de PC 3 a D1 y D2

PC4 debería hacer ping con éxito a:

- D1: 10.0.100.1

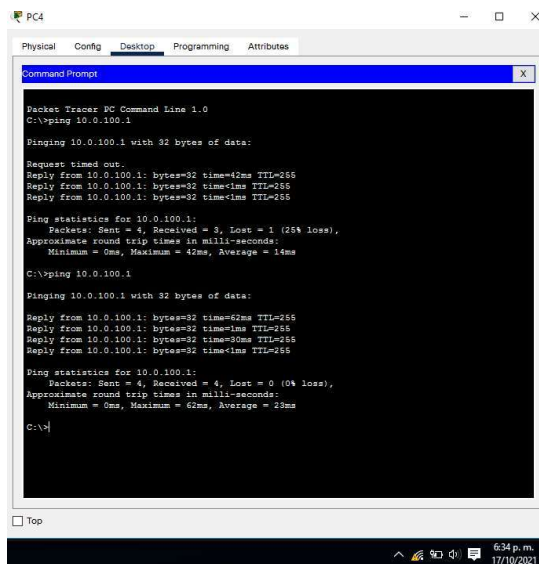


Ilustración 28 Ping de PC 4 a D1

- D2: 10.0.100.2

```

C:\>ping 10.0.100.1
Pinging 10.0.100.1 with 32 bytes of data:
Reply from 10.0.100.1: bytes=32 time=30ms TTL=255
Reply from 10.0.100.1: bytes=32 time<ms TTL=255

Ping statistics for 10.0.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 62ms, Average = 23ms

C:\>ping 10.0.100.2
Pinging 10.0.100.2 with 32 bytes of data:
Request timed out.
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.100.2
Pinging 10.0.100.2 with 32 bytes of data:
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Ilustración 29 Ping de PC 4 a D2

- PC1: 10.0.100.5

```

C:\>ping 10.0.100.2
Pinging 10.0.100.2 with 32 bytes of data:
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.100.2
Pinging 10.0.100.2 with 32 bytes of data:
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255
Reply from 10.0.100.2: bytes=32 time<ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.100.5
Pinging 10.0.100.5 with 32 bytes of data:
Reply from 10.0.100.5: bytes=32 time=40ms TTL=128
Reply from 10.0.100.5: bytes=32 time<ms TTL=128
Reply from 10.0.100.5: bytes=32 time<ms TTL=128
Reply from 10.0.100.5: bytes=32 time<ms TTL=128

Ping statistics for 10.0.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 40ms, Average = 17ms
  
```

Ilustración 30 Ping del PC4 al PC1

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.

Tabla 3 Configuración de los protocolos de enrutamiento

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.	<p>Use OSPF Process ID 4 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>Use OSPF Process ID 6 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 <p>En R1, R3, D1, y D2, anuncie todas las redesdirectamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP. <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. <p>En IPv6 address family:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

3.1 En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.

Use OSPF Process ID **4** y asigne los siguientes router-IDs:

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

- En R1, no publique la red R1 – R2.
- En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv2 en:

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

Deshabilite las publicaciones OSPFv2 en:

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

R1: 0.0.4.1

R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#router ospf 4

R1(config-router)#router-id 0.0.4.1

R1(config-router)#network 10.0.10.0 0.0.0.255 area 0

R1(config-router)#network 10.0.13.0 0.0.0.255 area 0

R1(config-router)#default-information originate

```
R1
R1#show ip protocols
Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 0.0.4.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.0.10.0 0.0.0.255 area 0
    10.0.13.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    0.0.4.1          110          00:01:28
  Distance: (default is 110)
```

Ilustración 31 Configuración OSPFv2 en area 0 de R1

R3: 0.0.4.3

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 4

R3(config-router)#router-id 0.0.4.3

R3(config-router)#network 10.0.11.0 0.0.0.255 area 0

R3(config-router)#network 10.0.13.0 0.0.0.255 area 0

R3(config-router)#

00:08:45: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Serial0/1/0 from
LOADING to FULL, Loading Done

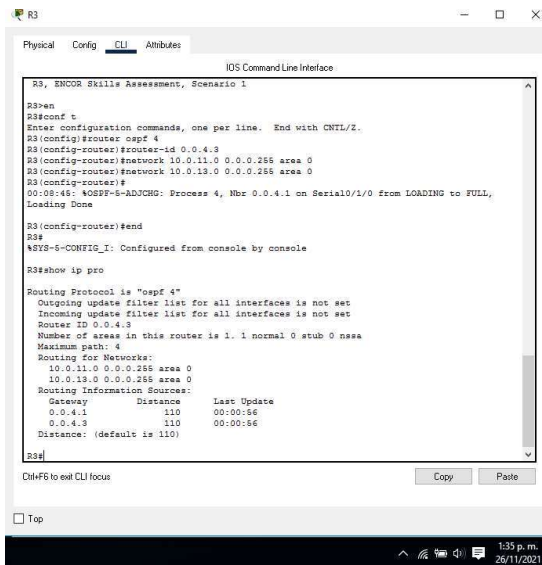


Ilustración 32 Configuración OSPFv2 en area 0 de R3

D1: 0.0.4.131

D1>en

D1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

D1(config)#router ospf 4

D1(config-router)#router-id 0.0.4.131

D1(config-router)#network 10.0.10.0 0.0.0.255 area 0

D1(config-router)#network 10.0.100.0 0.0.0.255 area 0

D1(config-router)#network 10.0.101.0 0.0.0.255 area 0

D1(config-router)#network 10.0.102.0 0.0.0.255 area 0

D1(config-router)#passive-interface g1/0/1

D1(config-router)#passive-interface g1/0/2

D1(config-router)#passive-interface g1/0/3

D1(config-router)#passive-interface g1/0/4

D1(config-router)#passive-interface g1/0/5

D1(config-router)#passive-interface g1/0/6

```
D1(config-router)#passive-interface g1/0/7
D1(config-router)#passive-interface g1/0/8
D1(config-router)#passive-interface g1/0/9
D1(config-router)#passive-interface g1/0/10
D1(config-router)#passive-interface g1/0/12
D1(config-router)#passive-interface g1/0/13
D1(config-router)#passive-interface g1/0/14
D1(config-router)#passive-interface g1/0/15
D1(config-router)#passive-interface g1/0/16
D1(config-router)#passive-interface g1/0/17
D1(config-router)#passive-interface g1/0/18
D1(config-router)#passive-interface g1/0/19
D1(config-router)#passive-interface g1/0/20
D1(config-router)#passive-interface g1/0/21
D1(config-router)#passive-interface g1/0/22
D1(config-router)#passive-interface g1/0/23
D1(config-router)#passive-interface g1/0/24
D1(config-router)#passive-interface g1/1/1
D1(config-router)#passive-interface g1/1/2
D1(config-router)#passive-interface g1/1/3
D1(config-router)#passive-interface g1/1/4
D1(config-router)#exit
```

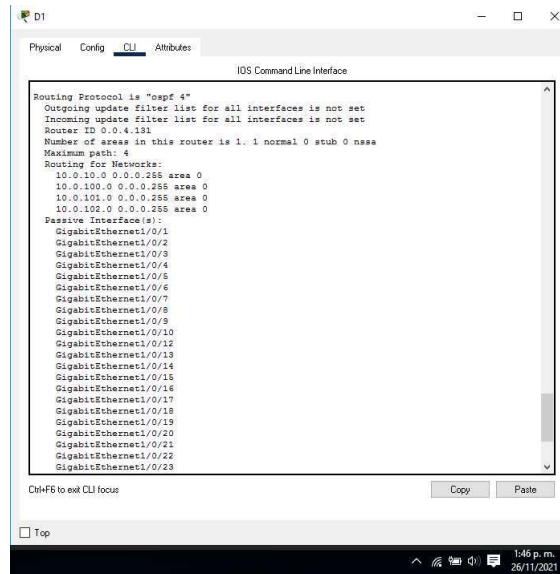


Ilustración 33 Configuración OSPFv2 en area 0 de D1

D2: 0.0.4.132

D2>en

D2#config t

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#router ospf 4

D2(config-router)#router-id 0.0.4.132

D2(config-router)#network 10.0.11.0 0.0.0.255 area 0

D2(config-router)#network 10.0.100.0 0.0.0.255 area 0

D2(config-router)#network 10.0.101.0 0.0.0.255 area 0

D2(config-router)#

00:24:39: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Vlan100 from LOADING to FULL, Loading Done

D2(config-router)#network 10.0.102.0 0.0.0.255 area 0

D2(config-router)#passive-interface g1/0/1

D2(config-router)#passive-interface g1/0/2

D2(config-router)#passive-interface g1/0/3

D2(config-router)#passive-interface g1/0/4

```
D2(config-router)#passive-interface g1/0/5
D2(config-router)#passive-interface g1/0/6
D2(config-router)#passive-interface g1/0/7
D2(config-router)#passive-interface g1/0/8
D2(config-router)#passive-interface g1/0/9
D2(config-router)#passive-interface g1/0/10
D2(config-router)#passive-interface g1/0/12
D2(config-router)#passive-interface g1/0/13
D2(config-router)#passive-interface g1/0/14
D2(config-router)#passive-interface g1/0/15
D2(config-router)#passive-interface g1/0/16
D2(config-router)#passive-interface g1/0/17
D2(config-router)#passive-interface g1/0/18
D2(config-router)#passive-interface g1/0/19
D2(config-router)#passive-interface g1/0/20
D2(config-router)#passive-interface g1/0/21
D2(config-router)#passive-interface g1/0/22
D2(config-router)#passive-interface g1/0/23
D2(config-router)#passive-interface g1/0/24
D2(config-router)#passive-interface g1/1/1
D2(config-router)#passive-interface g1/1/2
D2(config-router)#passive-interface g1/1/3
D2(config-router)#passive-interface g1/1/4
D2(config-router)#exit
```

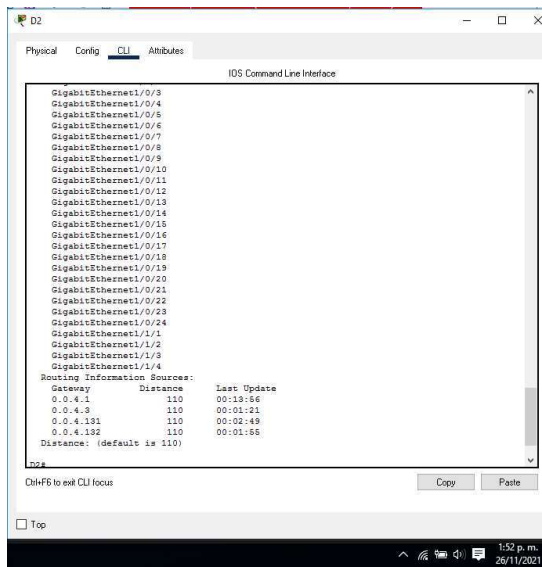


Ilustración 34 Configuración OSPFv2 en area 0 de D2

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

Use OSPF Process ID **6** y asigne los siguientes router-IDs:

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

- En R1, no publique la red R1 – R2.
- En R1, propague una ruta por defecto.

Note que la ruta por defecto deberá ser provista por BGP

Deshabilite las publicaciones OSPFv3 en:

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

R1: 0.0.6.1

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ipv6 router ospf 6

R1(config-rtr)#router-id 0.0.6.1

R1(config-rtr)#default-information originate

R1(config-rtr)#exit

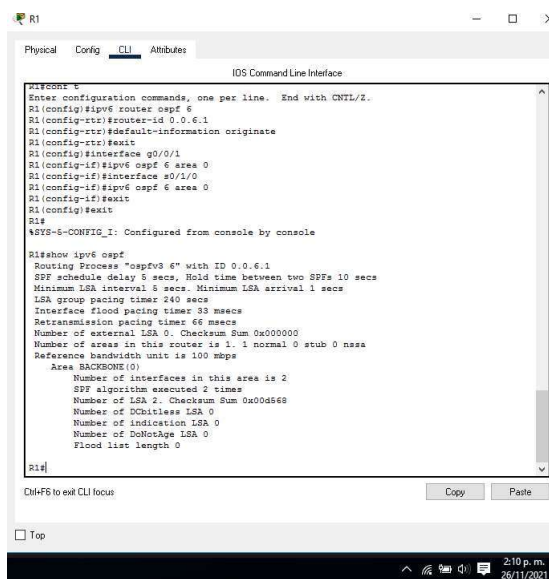
R1(config)#interface g0/0/1

R1(config-if)#ipv6 ospf 6 area 0

R1(config-if)#exit

R1(config-if)#interface s0/1/0

R1(config-if)#ipv6 ospf 6 area 0



```
R1
Physical  Config  CLI  Attributes
IOS Command Line Interface
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface g0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#interface s0/1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 ospf
Routing Process "ospfv3 6" With ID 0.0.6.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 8 secs, Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0, Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
Number of interfaces in this area is 2
SPF algorithm executed 2 times
Number of LSA 2, Checksum Sum 0x00d668
Number of DoNotAge LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
R1#
```

Ilustración 35 Configuración OSPFv3 en R1

R3: 0.0.6.3

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#ipv6 router ospf 6

R3(config-rtr)#router-id 0.0.6.3

R3(config-rtr)#exit

R3(config)#interface g0/0/1

R3(config-if)#ipv6 ospf 6 area 0

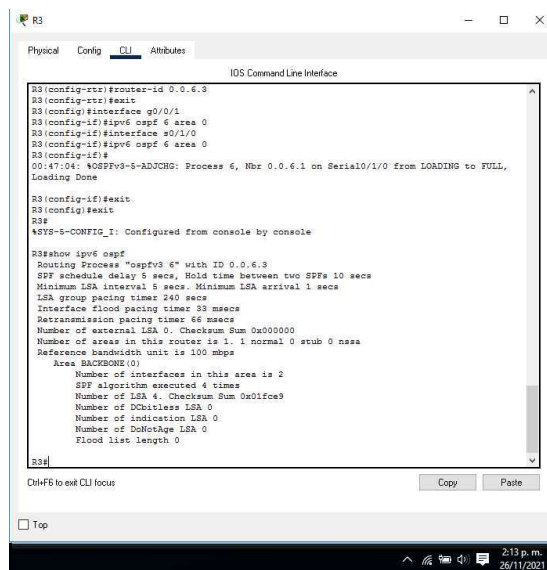
R3(config-if)#interface s0/1/0

```
R3(config-if)#ipv6 ospf 6 area 0
```

```
R3(config-if)#
```

```
00:47:04: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial0/1/0 from  
LOADING to FULL, Loading Done
```

```
R3(config-if)#exit
```



```
R3 (config-rtr)#router-id 0.0.6.3
R3 (config-rtr)#exit
R3 (config)#interface g0/0/1
R3 (config-if)#ipv6 ospf 6 area 0
R3 (config-if)#interface s0/1/0
R3 (config-if)#ipv6 ospf 6 area 0
R3 (config-if)#
00:47:04: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial0/1/0 from LOADING to FULL,
Loading Done
R3 (config-if)#exit
R3 (config)#exit
R3#
*SYS-5-CONFIG_I: Configured from console by console

R3#show ipvs ospf
Routing Process "ospfv3 6" with ID 0.0.6.3
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0, Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 2
  SPF algorithm executed 4 times
  Number of LSA 4, Checksum Sum 0x01fce9
  Number of DoNotAge LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
R3#
```

Ilustración 36 Configuración OSPFv3 en R3

```
D1: 0.0.6.131
```

```
D1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
D1(config)#ipv6 router ospf 6
```

```
D1(config-rtr)#router-id 0.0.6.131
```

```
D1(config-rtr)#exit
```

```
D1(config)#interface g1/0/11
```

```
D1(config-if)#ipv6 ospf 6 area 0
```

```
D1(config-if)#inter vlan100
```

```
00:50:33: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on GigabitEthernet1/0/11  
from LOADING to FULL, Loading Done
```

```
D1(config-if)#exit
```

```

D1(config)#inter vlan100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#inter vlan101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#inter vlan102
D1(config-if)#ipv6 ospf 6 area 0

```

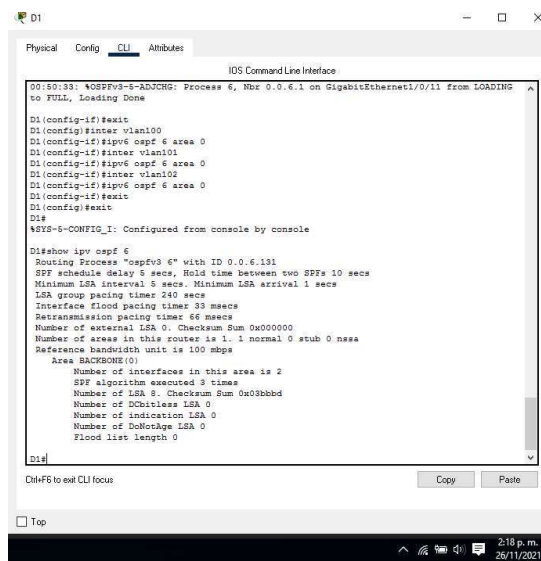


Ilustración 37 Configuración OSPFv3 en D1

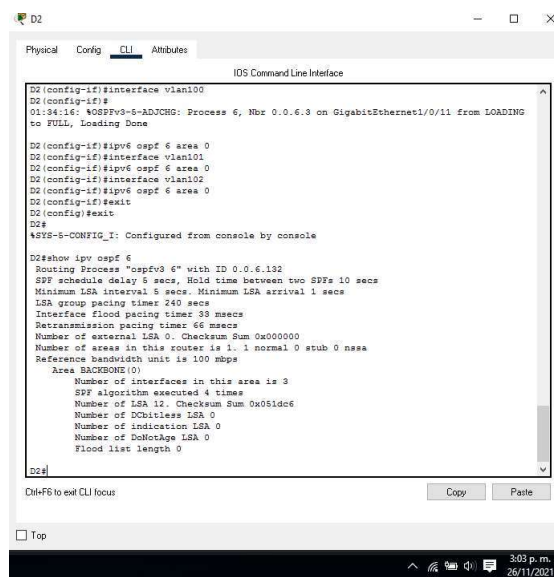
D2: 0.0.6.132

```

D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#exit
D2(config)#interface g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan100
D2(config-if)#ipv6 ospf 6 area 0

```

```
D2(config-if)#interface vlan101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
```



```
D2
D2 (config-if)#interface vlan100
D2 (config-if)#
01:34:16: %OSPFv3-6-ADJCHG: Process 6, Nbr 0.0.0.6.3 on GigabitEthernet1/0/11 from LOADING
to FULL, Loading Done
D2 (config-if)#ipv6 ospf 6 area 0
D2 (config-if)#interface vlan101
D2 (config-if)#ipv6 ospf 6 area 0
D2 (config-if)#interface vlan102
D2 (config-if)#ipv6 ospf 6 area 0
D2 (config-if)#exit
D2 (config-if)#exit
D2#
%SYS-5-CONFIG_I: Configured from console by console
D2#
D2#show ipv6 ospf 6
Routing Process "ospfv3 6" with ID 0.0.0.132
SPP schedule delay 5 secs, Hold time between two SPPs 10 secs
Minimum LSA interval 5 secs, Maximum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 39 msec
Retransmission pacing timer 66 msec
Number of external LSA 0, Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
  Area BACKBONE (0)
    Number of interfaces in this area is 3
    SPP algorithm executed 4 times
    Number of LSA 12, Checksum Sum 0x051dc6
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of Nullcost LSA 0
    Flood list length 0
D2#
Data+FB to exit CLI focus
```

Ilustración 38 Configuración OSPFv3 en D2

3.3 En R2 en la “Red ISP”, configure MP- BGP.

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.
- Una ruta estática predeterminada IPv6.

R2

```
R2>en
```

```
R2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
```

%Default route without gateway, if not a point-to-point interface, may impact performance

```
R2(config)#ipv6 route ::/0 loopback 0
```

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

Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

En IPv4 address family, anuncie:

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0).

En IPv6 address family, anuncie:

- La red Loopback 0 IPv4 (/128).
- La ruta por defecto (::/0).

R2

```
R2>en
```

```
R2#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
```

%Default route without gateway, if not a point-to-point interface, may impact performance

```
R2(config)#ipv6 route ::/0 loopback 0
```

```
R2(config)#router bgp 500
```

```
R2(config-router)#bgp router-id 2.2.2.2
```

```

R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
% Invalid input detected at '^' marker. // Comando no Soportado
R2(config-router)#address-family ipv4 unicast
% Invalid input detected at '^' marker. // Comando no Soportado
R2(config-router)#network 2.2.2.2 mask 255.255.255.255
R2(config-router)#network 0.0.0.0 mask 0.0.0.0

```

Los comandos que se utilizan son los siguientes en caso de ser soportado:

```

R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4 “Se asigna la familia a ipv4”
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6 “Se asigna a la familia a ipv6”
R2(config-router-af)#no neighbor 209.165.200.225 activate “ Se activa el modo vecino en ipv4”
R2(config-router-af)#neighbor 2001:db8:200::1 activate “Se activa el modo vecino en ipv6”
R2(config-router-af)#network 2001:db8:2222::/128 R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family

```

Se empleará el simulador, en el cual se explicará diseño e implementación de soluciones integradas, donde se trabajará una serie de elementos tales como, switch, router, diferentes tipos de cables, donde abra conexión entre servidores, nube y demás para así dar como resultado las configuraciones entre DNS y permitiendo el acceso a la red y los recursos que se pueden llegar a manejar entre sí.

Las redes de datos, características que están traen, además que se usan a través de nuestra vida cotidiana son ofrecidas a través de una simulación con la cual podemos llegar a realizar diversos protocolos, realizar el análisis a profundidad para determinar el comportamiento que esta se ejecuta.

Conectividades exitosas.

El protocolo OSPF sirve para simplificar las rutas ya que siempre se elige la ruta más corta de conexión.

Es un protocolo de encaminamiento muy útil cuando se tiene circuitos redundantes en una red mejora los tiempos.

Se puede priorizar o darle mayor importancia a una red o ruta.

Las listas de acceso mejoran los rendimientos por que se pueden programar las rutas.

Las listas de accesos son inclusivas y exclusivas.

Con esta forma de enrutamiento podemos restringir el acceso de los usuarios y se pueden aprovechar de una mejor manera los recursos.

Las listas de acceso mejoran los rendimientos por que se pueden programar las rutas.

Las listas de accesos son inclusivas y exclusivas.

Con esta forma de enrutamiento podemos restringir el acceso de los usuarios y se pueden aprovechar de una mejor manera los recursos.

Se concluye que gracias a las ACL nos da la posibilidad de permitir o denegar claro está que las Access-list se pueden aplicar en muchos más escenarios inclusive con protocolos y esto nos permite dar un mejor manejo de la red, esto dependiendo la necesidad del cliente o solución que debamos implementar como futuros ingenieros de redes o networking.

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.

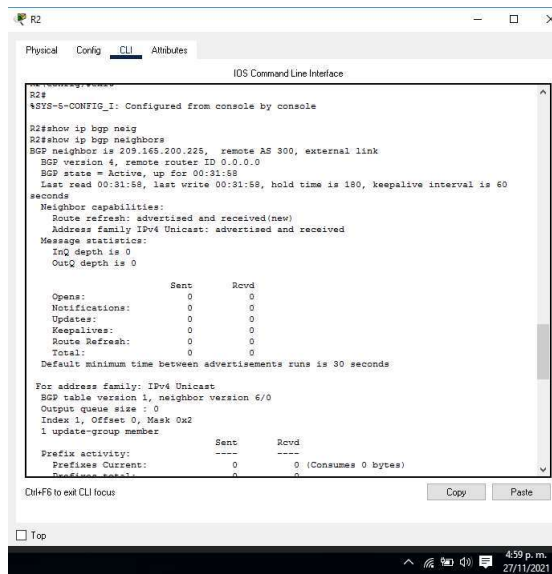


Ilustración 39 verificación configuración BGP mediante el comando (Show ip BGP neighbor) en R3

3.4 En R1 en la “Red ISP”, configure MP- BGP.

Configure dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.
- Una ruta resumen IPv6 para 2001:db8:100::/48.

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

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

- Deshabilite la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.
- Anuncie la red 10.0.0.0/8.

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.
- Anuncie la red 2001:db8:100::/48.

R1

R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip route 10.0.0.0 255.0.0.0 null0

%Default route without gateway, if not a point-to-point interface, may impact performance

R1(config)#ipv6 route 2001:db8:100::/48 null0

% Invalid input detected at '^' marker.

R1(config)#router bgp 300

R1(config-router)#bgp router-id 1.1.1.1

R1(config-router)#neighbor 209.165.200.226 remote-as 500

R1(config-router)#%BGP-5-ADJCHANGE: neighbor 209.165.200.226 Up

R1(config-router)#neighbor 2001:db8:200::2 remote-as 500

^

% Invalid input detected at '^' marker. // **Comando no soportado**

R1(config-router)#address-family ipv4 unicast

^

% Invalid input detected at '^' marker. // **Comando no soportado**

Los comandos que se utilizan son los siguientes en caso de ser soportado:

R1(config-router)#neighbor 2001:db8:200::2 remote-as 500

R1(config-router)#address-family ipv4 unicast *“Se activa la dirección ipv4”*

R1(config-router-af)#neighbor 209.165.200.226 activate *“Se activa el modo vecino en ipv4”*

R1(config-router-af)#no neighbor 2001:db8:200::2 activate *“Se activa el modo vecino en ipv6”*

R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0 “Muestra la máscara subred”

R1(config-router-af)#exit-address-family

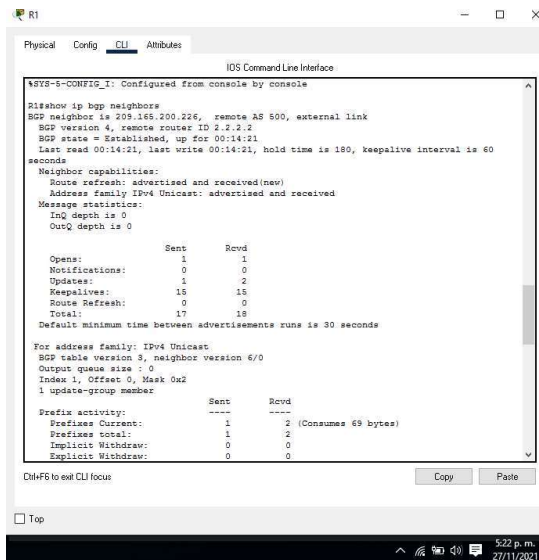
R1(config-router)#address-family ipv6 unicast

R1(config-router-af)#no neighbor 209.165.200.226 activate R1(config-router-af)#neighbor 2001:db8:200::2 activate

R1(config-router-af)#network 2001:db8:100::/48

R1(config-router-af)#exit-address-family

R1(config-router)#



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1S13-S-CONF10_1: Configured from console by console
R1#show ip bgp neighbors
BGP neighbor is 209.165.200.226, remote AS 500, external link
  BGP version 4, remote router ID 2.2.1.2
  BGP state = Established, up for 00:14:21
  Last read 00:14:21, last write 00:14:21, hold time is 180, keepalive interval is 60
  seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0
      Sent      Rcvd
Opens:          1          1
Notifications: 0          0
Updates:        1          2
Keepalives:     15         15
Route Refresh:  0          0
Total:          17         18
Default minimum time between advertisements runs is 30 seconds
For address family: IPv4 Unicast
  BGP table version 3, neighbor version 6/0
  Output queue size 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
Prefix activity:
      Sent      Rcvd
Prefixes Current: 1          2 (Consumes 69 bytes)
Prefixes total:   1          2
Implicit Withdraw: 0          0
Explicit Withdraw: 0          0
Ctrl+F8 to exit CLI focus
Copy Paste
Top
5:22 p.m.
27/11/2021
```

Ilustración 40 verificación configuración BGP mediante el comando (Show ip BGP neighbor) en R1

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

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

Tabla 4 Configuración de la Redundancia del Primer Salto (First Hop Redundancy)

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none">• Use la SLA número 4 para IPv4.• Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none">• Use el número de rastreo 4 para la IP SLA 4.• Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none">• Use la SLA número 4 para IPv4.• Use la SLA número 6 para IPv6. <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none">• Use el número de rastreo 4 para la IP SLA 4.• Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • 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. <p>D2 es el router primario para la VLAN 101; por lo tanto, su</p>
-----	-------------------------	---

	<p>En D2 configure HSRPv2.</p>	<p>prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). <p>Rastree el objeto 6 para disminuir en 60</p>
--	--------------------------------	---

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

Cree dos IP SLAs.

- Use la SLA número **4** para IPv4.
- Use la SLA número **6** para IPv6.

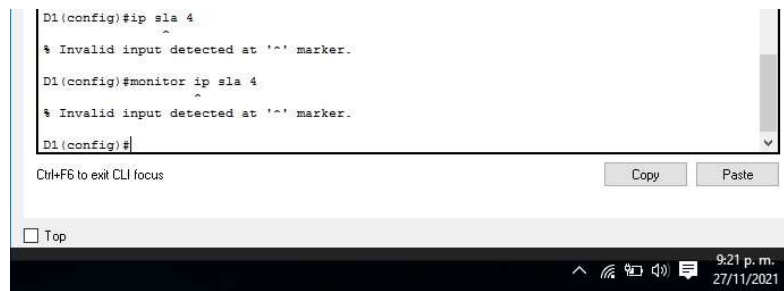
Las IP SLAs probarán la disponibilidad de la interfaz R1G0/0/1 cada 5 segundos.

Programe la SLA para una implementación inmediata sintiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6.

- Use el número de rastreo **4** para la IP SLA 4.
- Use el número de rastreo **6** para la IP SLA 6.

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



```
D1(config)#ip sla 4
% Invalid input detected at '^' marker.
D1(config)#monitor ip sla 4
% Invalid input detected at '^' marker.
D1(config)#
```

Ilustración 41 Comando SLAs no soportado por packet Tracer

D1

```
D1(config)#ip sla 4
```

```
% Invalid input detected at '^' marker.
```

```
D1(config)#monitor ip sla 4
```

```
% Invalid input detected at '^' marker.
```

```
D1(config)#
```

Los comandos que se utilizan son los siguientes en caso de ser soportado:

Se debe ingresar al modo de configuración global.

D1#configure terminal “ Se configura la terminal en este caso el equipo”

D1(config)#ip sla 4 “ con sla 4 activamos la prueba de disponibilidad de la interfaz R1G0/0/1 cada 5 segundos. En ipv 4”

D1(config-ip-sla)#icmp-echo 10.0.10.1 source-interface e2/1 “ se realiza la configuración de dirección ipv 4 de monitoreo desde la que realizamos”

D1(config-ip-sla-echo)# frequency 5 “ es la frecuencia con la que se hará monitoreo en este caso 5 min”

D1(config)#ip sla schedule 4 start-time now life forever “la operación 4 está configurada para ejecutarse indefinidamente y programada para comenzar inmediatamente”

D1(config)#track 4 ip sla 4 state “Realiza el seguimiento del estado de la operación para este caso el ID de objeto 4 se crea y se asocia con la operación 4”

D1(config-track)#delay up 10 down 15 “notificación de retardo de down y up”

D1(config-track)#exit “salida de la configuración track”

D1(config)#ip sla 6 “ con sla 6 activamos la prueba de disponibilidad de la interfaz R1G0/0/1 cada 5 segundos. En ipv 6”

D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-interface e2/1 “ se realiza la configuración de dirección ipv 6 de monitoreo desde la que realizamos”

D1(config-ip-sla-echo)#frequency 5 “ es la frecuencia con la que se hará monitoreo en este caso 5 min”

D1(config-ip-sla-echo)#exit “ salida del modo configuración de sla”

D1(config)#ip sla schedule 6 start-time now life forever “la operación 6 está configurada para ejecutarse indefinidamente y programada para comenzar inmediatamente”

D1(config)#track 6 ip sla 6 “Realiza el seguimiento del estado de la operación para este caso el ID de objeto 4 se crea y se asocia con la operación 4”

D1(config-track)#delay up 10 down 15 “notificación de retardo de down y up”

D1(config-track)#exit “ salida de la configuración track”

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

Cree IP SLAs.

- Use la SLA número 4 para IPv4.

- Use la SLA número **6** para IPv6.

Las IP SLAs probarán la disponibilidad de la interfaz R3G0/0/1 cada 5 segundos.

Programa la SLA para una implementación inmediata sintiendo de finalización.

Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 6.

- Use el número de rastreo **4** para la IP SLA 4.
- Use el número de rastreo **6** para la SLA 6.

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

```

D2>en
D2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ip sla 4
% Invalid input detected at '^' marker.
D2(config)#
  
```

Ilustración 42 Comando SLAs no soportado por packet Tracer en D2

Los comandos que se utilizan son los siguientes en caso de ser soportado:

Se debe ingresar al modo de configuración global.

D2#configure terminal “ Se configura la terminal en este caso el equipo”

D2 (config)#ip sla 4 “ con sla 4 activamos la prueba de disponibilidad de la interfaz R1G0/0/1 cada 5 segundos. En ipv 4”

D2(config-ip-sla)#icmp-echo 10.0.10.1 source-interface e2/1 “ se realiza la configuración de dirección ipv 4 de monitoreo desde la que realizamos”

D2(config-ip-sla-echo)# frequency 5 “ es la frecuencia con la que se hará monitoreo en este caso 5 min”

D2(config)#ip sla schedule 4 start-time now life forever “la operación 4 está configurada para ejecutarse indefinidamente y programada para comenzar inmediatamente”

D2(config)#track 4 ip sla 4 state *“Realiza el seguimiento del estado de la operación para este caso el ID de objeto 4 se crea y se asocia con la operación 4”*

D2(config-track)#delay up 10 down 15 *“notificación de retardo de down y up”*

D2(config-track)#exit *“salida de la configuración track”*

D2(config)#ip sla 6 *“ con sla 6 activamos la prueba de disponibilidad de la interfaz R1G0/0/1 cada 5 segundos. En ipv 6”*

D2(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-interface e2/1 *“ se realiza la configuración de dirección ipv 6 de monitoreo desde la que realizamos”*

D2(config-ip-sla-echo)#frequency 5 *“ es la frecuencia con la que se hará monitoreo en este caso 5 min”*

D2(config-ip-sla-echo)#exit *“ salida del modo configuración de sla”*

D2(config)#ip sla schedule 6 start-time now life forever *“la operación 6 está configurada para ejecutarse indefinidamente y programada para comenzar inmediatamente”*

D2(config)#track 6 ip sla 6 *“Realiza el seguimiento del estado de la operación para este caso el ID de objeto 4 se crea y se asocia con la operación 4”*

D2(config-track)#delay up 10 down 15 *“notificación de retardo de down y up”*

D2(config-track)#exit *“ salida de la configuración track”*

4.3 En D1 y D2 configure HSRPv2.

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

Configure HSRP versión 2.

Configure IPv4 HSRP grupo **104** para la VLAN 100:

- Asigne la dirección IP virtual **10.0.100.254**.
- Establezca la prioridad del grupo en **150**.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

D1

D1(config)#interface vlan 100

```

D1(config-if)#standby version 2
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 track 4 decrement 60
% Invalid input detected at '^' marker. “Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
D1(config-if)#exit

```

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.

D1

```

D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#interface vlan 101
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
D1(config-if)#standby 114 preempt
D1(config-if)#standby version 2
D1(config-if)#
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Active -> Init
D1(config-if)#standby 114 track 4 decrement 60
% Invalid input detected at '^' marker. “Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
D1(config-if)#end

```

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.

```
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 track 4 decrement 60
% Invalid input detected at '^' marker. “Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#exit
```

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.

```
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
```

% Invalid input detected at '^' marker. **“Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”**

```
D1(config-if)#standby ipv6 autoconfig
D1(config-if)#exit
```

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.

```
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
% Invalid input detected at '^' marker. “ Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
D1(config-if)#end
```

Configure IPv6 HSRP grupo **126** para la VLAN 102:

- Asigne la dirección IP virtual usando **ipv6 autoconfig**.
- Establezca la prioridad del grupo en **150**.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 y decremente en 60.

```
D1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
% Invalid input detected at '^' marker. “ Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
D1(config-if)#standby 126 priority 150
D1(config-if)#exit
```

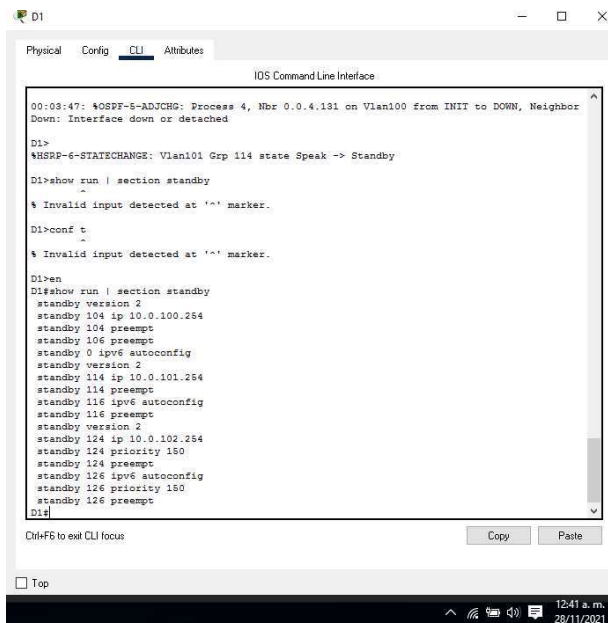


Ilustración 43 Verificación standby en D1

D2 es el router primario para la VLAN 101; por lo tanto, superioridad también se cambiará a 150.

Configure HSRP version 2.

Configure IPv4 HSRP grupo **104** para la VLAN 100:

- Asigne la dirección IP virtual **10.0.100.254**.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

D2#configure terminal

D2(config)#interface vlan 100

D2(config-if)#standby version 2

D2(config-if)#standby 104 ip 10.0.100.254

D2(config-if)#standby 104 preempt

D2(config-if)#standby 104 track 4 decrement 60

% Invalid input detected at '^' marker. **“Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”**

D2(config-if)#end

Configure IPv4 HSRP grupo **114** para la VLAN 101:

- 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.

D2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#interface vlan 101

D2(config-if)#standby version 2

D2(config-if)#standby 114 ip 10.0.101.254

D2(config-if)#standby 114 priority 150

D2(config-if)#standby 114 preempt

D2(config-if)#standby 114 track 4 decrement 60

% Invalid input detected at '^' marker. **“Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”**

D2(config-if)#exit

Configure IPv4 HSRP grupo **124** para la VLAN 102:

- Asigne la dirección IP virtual **10.0.102.254**.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

D2(config)#interface vlan 102

D2(config-if)#standby version 2

D2(config-if)#standby 124 ip 10.0.102.254

D2(config-if)#standby 124 preempt

D2(config-if)#standby 124 track 4 decrement 60

% Invalid input detected at '^' marker. **“ Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”**

D2(config-if)#end

Configure IPv6 HSRP grupo **106** para la VLAN 100:

- Asigne la dirección IP virtual usando **ipv6 autoconfig**.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

```
D2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
D2(config)#interface vlan 100
```

```
D2(config-if)#standby version 2
```

```
D2(config-if)#standby 106 ipv6 autoconfig
```

```
D2(config-if)#standby 106 preempt
```

```
D2(config-if)#standby 106 track 6 decrement 60
```

```
% Invalid input detected at '^' marker. “ Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
```

```
D2(config-if)#end
```

Configure IPv6 HSRP grupo **116** para la VLAN 101:

- Asigne la dirección IP virtual usando **ipv6 autoconfig**.
- Establezca la prioridad del grupo en **150**.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

```
D2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
D2(config)#interface vlan 101
```

```
D2(config-if)#standby version 2
```

```
D2(config-if)#standby 116 priority 150
```

```
D2(config-if)#standby 116 preempt
```

```
D2(config-if)#standby 116 track 6 decrement 60
```

```
% Invalid input detected at '^' marker. “ Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”
```

```
D2(config-if)#standby 116 ipv6 autoconfig
```

```
% Group configured for different address family
```

```
D2(config-if)#end
```

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.

D2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#interface vlan 102

D2(config-if)#standby version 2

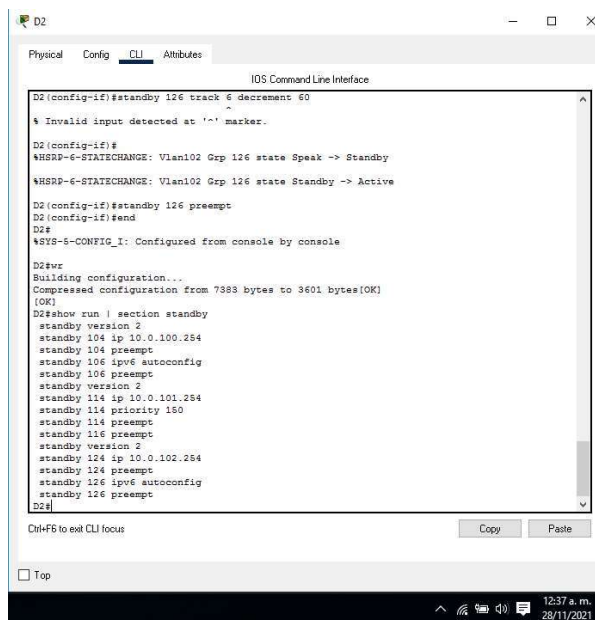
D2(config-if)#standby 126 ipv6 autoconfig

D2(config-if)#standby 126 track 6 decrement 60

% Invalid input detected at '^' marker. **“Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para el rastreo del objeto con disminución en 60”**

D2(config-if)#standby 126 preempt

D2(config-if)#end



```
D2 (config-if)#standby 126 track 6 decrement 60
% Invalid input detected at '^' marker.
D2 (config-if)#
%HSRP-6-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan102 Grp 126 state Standby -> Active
D2 (config-if)#standby 126 preempt
D2 (config-if)#end
D2#
%SYS-5-CONFIG_I: Configured from console by console

D2#wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
D2#show run | section standby
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 106 ipv6 autoconfig
standby 106 preempt
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 116 preempt
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 126 ipv6 autoconfig
standby 126 preempt
D2#
```

Ilustración 44 Verificación standby en D2

Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Tabla 5 Configuración de Seguridad

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: <ul style="list-style-type: none"> Nombre de usuario Local: sadmin Nivel de privilegio 15 Contraseña: cisco12345cisco
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <ul style="list-style-type: none"> Dirección IP del servidor RADIUS es 10.0.100.6. Puertos UDP del servidor RADIUS son 1812 y 1813. Contraseña: \$strongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> Use la lista de métodos por defecto Valide contra el grupo de servidores RADIUS De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (excepto R2).	Cierre e inicie sesión en todos los dispositivos (excepto R2) con el usuario: raduser y la contraseña: upass123 .

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

Contraseña: **cisco12345cisco**

R1

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#enable algorithm-type scrypt secret cisco12345cisco

% Invalid input detected at '^' marker. **“Se ejecutó el siguiente comando el cual no funciona correctamente debido a problemas de compatibilidad, por lo tanto este comando es utilizado para ser difícil de implementar en paralelo en GPU y ASIC esto significa que no cualquier atacante ingrese con facilidad a la contraseña puesta”**

Nota: El comando algorithm-type Scrypt, no será soportado en los siguientes router y switch también como lo son: R2, R3, D1, D2 y A1.

Para este caso utilizaremos los siguientes comandos como se muestran a continuación:

R1

R1>en

R1#config t

R1(config)#enable secret cisco12345cisco

R1(config)#service password-encryption

R1(config)#exit

R2

R2>en

R2#config t

R2(config)#enable secret cisco12345cisco

R2(config)#service password-encryption

R2(config)#exit

R3

R3>en

R3#config t

R3(config)#enable secret cisco12345cisco

R3(config)#service password-encryption

R3(config)#exit

D1

D1>en

D1#config t

D1(config)#enable secret cisco12345cisco

D1(config)#service password-encryption

D1(config)#exit

D2

D2>en

D2#config t

D2(config)#enable secret cisco12345cisco

D2(config)#username sadmin privilege 15 secret

D2(config)#service password-encryption

D2(config)#exit

A1

A1>en

A1#config t

```
A1(config)#enable secret cisco12345cisco
```

```
A1(config)#service password-encryption
```

```
A1(config)#exit
```

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

Detalles de la cuenta encriptada SCRYPT:

- Nombre de usuario Local: **sadmin**
- Nivel de privilegio **15**
- Contraseña: **cisco12345cisco**

R1

```
R1#config t
```

```
R1(config)#enable secret level 15 cisco12345cisco
```

```
R1(config)#username sadmin privilege 15 secret cisco12345cisco
```

R2

```
R2(config)#enable secret level 15 cisco12345cisco
```

```
R2(config)#username sadmin privilege 15 secret cisco12345cisco
```

R3

```
R3(config)#enable secret level 15 cisco12345cisco
```

```
R3(config)#username sadmin privilege 15 secret cisco12345cisco
```

D1

```
D1(config)#enable secret level 15 cisco12345cisco
```

```
D1(config)#username sadmin privilege 15 secret cisco12345cisco
```

D2

```
D2(config)#enable secret level 15 cisco12345cisco
```

```
D2(config)#username sadmin privilege 15 secret cisco12345cisco
```

A1

```
A1(config)#enable secret level 15 cisco12345cisco
```

```
A1(config)#username sadmin privilege 15 secret cisco12345cisco
```

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

Habilite AAA.

R1

R1(config)#aaa new-model

R3

R1(config)#aaa new-model

D1

D1(config)#aaa new-model

D2

D2(config)#aaa new-model

A1

A1(config)#aaa new-model

5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

Especificaciones del servidor RADIUS.:

- Dirección IP del servidor RADIUS es 10.0.100.6.
- Puertos UDP del servidor RADIUS son 1812 y 1813.
- Contraseña: **\$strongPass**

Nota: En los dispositivos R1, R3, D1, D2 y A1 no fue posible realizar la configuración ya que arroja error la configuración de packet Tracer, pero son los códigos para utilizar en un escenario simulado serían los correspondientes.

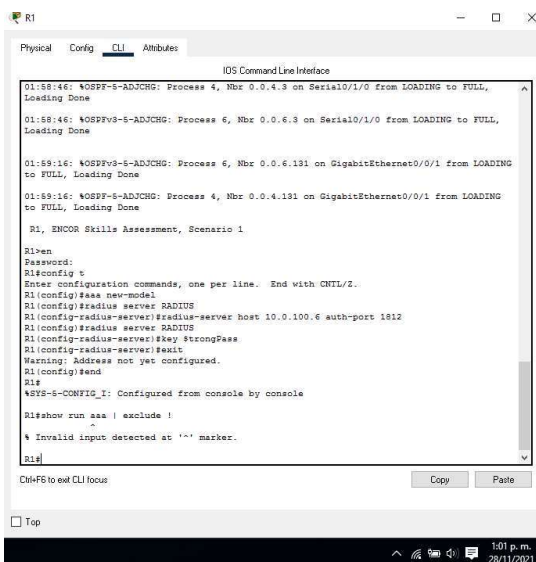
R1

R1(config)#radius server RADIUS *“ indica el servidor a configurar para este caso RADIUS”*

R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 *“se asigna la dirección ip y puertos del servidor Radius y los puertos UDP”*

R1(config-radius-server)#key \$trongPass “se asigna la contraseña para el ingreso al servidor RADIUS”

Esta configuración se debe aplicar al resto de los dispositivos R3, D1, D2 y A1. Se utilizan los mismos comandos exactamente.



```
R1
Physical Config CLI Attributes
IOS Command Line Interface
01:58:46: %OSPFV3-S-ADJCHG: Process 4, Nbr 0.0.4.3 on Serial0/1/0 from LOADING to FULL, Loading Done
01:58:46: %OSPFV3-S-ADJCHG: Process 6, Nbr 0.0.6.3 on Serial0/1/0 from LOADING to FULL, Loading Done
01:58:16: %OSPFV3-S-ADJCHG: Process 6, Nbr 0.0.6.131 on GigabitEthernet0/0/1 from LOADING to FULL, Loading Done
01:58:16: %OSPFV3-S-ADJCHG: Process 4, Nbr 0.0.4.131 on GigabitEthernet0/0/1 from LOADING to FULL, Loading Done
R1, EMCOR Skills Assessment, Scenario 1
R1>en
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#radius-server host 10.0.100.6 auth-port 1812
R1(config)#radius server RADIUS
R1(config-radius-server)#key StrongPass
R1(config-radius-server)#exit
Warning: Address not yet configured.
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show run aaa | exclude |
^
% Invalid input detected at '^' marker.
R1#
```

Ilustración 45 Validación de la configuración Server RADIUS

5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

Especificaciones de autenticación AAA:

- Use la lista de métodos por defecto
- Valde contra el grupo de servidores RADIUS
- De lo contrario, utilice la base de datos local.

Nota: En los dispositivos R1, R3, D1, D2 y A1 no fue posible realizar la configuración ya que arroja error la configuración de packet Tracer, pero son los códigos para utilizar en un escenario simulado serían los correspondientes.

R1

R1#configure terminal “Se ingresa a la configuración del terminal”

R1 (config)#AAA authentication login default group radius local “ con este comando realizamos la configuración del grupo RADIUS por defecto o de lo

contrario la configuración local”.

Esta configuración se debe aplicar al resto de los dispositivos R3, D1, D2 y A1. Se utilizan los mismos comandos exactamente.

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

Cierre e inicie sesión en todos los dispositivos (Except R2) con el usuario: **raduser** y la contraseña: **upass123**.

Nota: No se puede realizar la verificación del servicio AAA en los dispositivos debido a que no fue posible realizar la configuración correspondiente.

Verificar el servicio AAA (Authentication, Authorization, Accounting) permite el acceso de los usuarios legítimos a los activos conectados a la red e impide el acceso no autorizado de aquellos que quieran infringir el acceso no autorizado.

Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tabla 6 Configuración de las funciones de Administración de la RED

Tarea#	Tarea	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.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none">• R1 debe sincronizar con R2.• R3, D1 y A1 para sincronizar la hora con R1.• D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

6.5	Configure SNMPv2c en todos los dispositivos excepto R2	<p>Especificaciones de SNMPv2:</p> <ul style="list-style-type: none"> • Únicamente se usará SNMP en modo lectura(Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el <i>community string</i> en ENCORSA. • En R3, D1, y D2, habilite el envío de <i>trapsconfig</i> y <i>ospf</i>. • En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>. • En A1, habilite el envío de <i>traps config</i>.
-----	--	---

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

Configure el reloj local a la hora UTC actual.

R1

```
R1#clock set 01:15:00 28 nov 2021
```

```
R1#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#clock timezone UTC -5
```

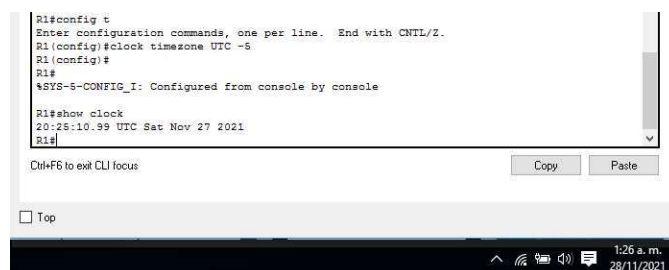


Ilustración 46 Configuración hora en R1

R2

R2#clock set 01:15:00 28 nov 2021

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#clock timezone UTC -5

R2(config)#exit

R2#show clock

20:15:21.568 UTC Sat Nov 27 2021

R3

R3>en

R3#clock set 01:33:00 28 nov 2021

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#clock timezone UTC -5

R3(config)#exit

R3#show clock

20:33:35.372 UTC Sat Nov 27 2021

D1

D1#clock set 01:15:00 28 nov 2021

D1#config t

Enter configuration commands, one per line. End with CNTL/Z.

D1(config)#clock timezone UTC -5

D1(config)#exit

D1#show clock

20:15:55.101 UTC Sat Nov 27 2021

D2

D2#clock set 01:15:00 28 nov 2021

D2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#clock timezone UTC -5

D2(config)#exit

D2#show clock

20:15:39.546 UTC Sat Nov 27 2021

A1

A1>en

A1#clock set 01:15:00 28 nov 2021

A1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

A1(config)#clock timezone UTC -5

A1(config)#exit

A1#show clock

20:15:23.623 UTC Sat Nov 27 2021

6.2 Configure R2 como un NTPmaestro.

Configurar R2 como NTP maestro en el nivel deestrato 3.

R2

R2(config)#ntp master 3

6.3 Configure NTP en R1, R3, D1, D2,y A1.

Configure NTP de la siguiente manera:

- R1 debe sincronizar con R2.
- R3, D1 y A1 para sincronizar la hora con R1.
- D2 para sincronizar la hora con R3.

R1

R1 sincronización con R2

```
R1#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#ntp server 209.165.200.226
```



Ilustración 47 Verificación NTP en R1

R3

R3 sincronización con R1

```
R3#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)#ntp server 10.0.13.1
```

```
R3(config)#end
```

D1 sincronización con R1

```
D# config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
D1(config)#ntp server 10.0.10.1
```

```
D1(config)#end
```

A1 Sincronización con R1

```
A1#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
A1(config)#ntp server 10.0.10.1
```

```
A1(config)#end
```

D2 Sincronización con R3.

D2#config t

Enter configuration commands, one per line. End with CNTL/Z.

D2(config)#ntp server 10.0.11.1

D2(config)#end

6.4 Configure Syslog en todos los dispositivos excepto R2

Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

Nota: En los dispositivos R1, R3, D1, D2 y A1 no fue posible realizar la configuración ya que arroja error la configuración de packet Tracer, pero son los códigos para utilizar en un escenario simulado serían los correspondientes.

R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#logging 10.0.100.5 “ Se realiza la configuración host Syslog”

R1(config)#logging trap warnings “Se realiza la configuración nivel warning

Esta configuración se debe aplicar al resto de los dispositivos R3, D1, D2 y A1. Se utilizan los mismos comandos exactamente.

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

- Únicamente se usará SNMP en modo lectura(Read-Only).
- Limite el acceso SNMP a la dirección IP de la PC1.
- Configure el valor de contacto SNMP con sunombre.
- Establezca el *community string* en **ENCORSA**.
- En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*.
- En R1, habilite el envío de *traps bgp*, *config*, y *Ospf*.
- En A1, habilite el envío de *traps config*.

Nota: En los dispositivos R1, R3, D1, D2 y A1 no fue posible realizar la configuración ya que arroja error la configuración de packet Tracer, pero son los códigos para utilizar en un escenario simulado serían los correspondientes.

```
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#permit host 10.0.100.5 R1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco student
R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config- snmp)#snmp-server ifindex persist R1(config- snmp)#snmp-server
enable traps config
R1(config- snmp)#snmp-server enable traps ospf
```

Nota: Esta configuración realizada en los dispositivos configurados no funciona con el comando snmp-server debido a que Packet Tracer no los recibe.

CONCLUSIONES

Se puede evidenciar el trabajo realizado a lo largo del diplomado, poniendo a prueba el enrutamiento y sincronización de los routers, el manejo de los ipv4 e ipv6. Al desarrollar e implementar los protocolos de la red, para el cambio de información y tráfico de datos, se genera la completa sincronización y conexión entre la red y sus routers o switches, con el fin de tener no solo conocimiento de ubicación y direccionamiento IP de estas, sino además conocer su estado, el envío y recepción de información y un control de seguridad.

Trabajar con el simulador Packet Tracer para este tipo de configuraciones tiene sus desventajas, puesto que varios de los comandos no son aceptados debido a las imágenes que tienen configurados los equipos y los cuales trae por defecto. Se recomienda el uso de otro simulador, para la configuración de los dispositivos, en este caso no fue posible realizar la del servidor RADIUS entre otras funciones.

Por medio de la realización del montaje de una red ISP BGP ASN500 se aplican presentan una serie de posibles comandos para la configuración de los protocolos dhcp, ospfv2, nat y vlan, así mismo se logró realizar la configuración de nombres, direcciones IP, claves de acceso de cada uno de los dispositivos activos de red y las interfaces, servidores, switch, pc y router

De igual manera con este diplomado se logró brindar solución al escenario propuesto de una red ISP partiendo desde una problemática de la vida cotidiana, afianzando los conocimientos para la carrera ingeniería en telecomunicaciones.

BIBLIOGRAFÍA

Es.wikipedia.org. 2021. Protocolo de configuración dinámica de host - Wikipedia, la enciclopedia libre. [Online] Recuperado de: https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host.

Es.wikipedia.org. 2021. Router - Wikipedia, la enciclopedia libre. [Online] Recuperado de: <https://es.wikipedia.org/wiki/Router#:~:text=Un%20r%C3%BAter%2C%E2%80%8B%20enrutador%2C%E2%80%8B,dentro%20de%20una%20red%20inform%C3%A1tica>.

Es.wikipedia.org. 2021. Proveedor de servicios de Internet - Wikipedia, la enciclopedia libre. [Online] Recuperado de: https://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

Reuter.com.ar. 2021. Documento sin título. [Online] Recuperado de: https://www.reuter.com.ar/CCNA/CCNA2/mod3_ccna2/.

Raponi, D., 2021. Cómo configurar el protocolo de enrutamiento de espera activa (HSRP) con un router Cisco | The Solving. [online] The Solving. Recuperado de: <https://thesolving.com/es/sala-de-servidores/como-configurar-hot-standby-router-protocol-hsrp-con-un-router-cisco#:~:text=La%20principal%20caracter%C3%ADstica%20del%20HSRP,virtual%20seguir%C3%A1%20siendo%20la%20misma>.

Redestematicas.com. 2021. El switch: cómo funciona y sus principales características | Redes Telemáticas. [Online] Recuperado de: <https://redestematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/>

Static-course-assets.s3.amazonaws.com. 2021. 10.2.1.1 Configuración automática de dirección sin estado (SLAAC). [Online] Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/10.2.1.1/10.2.1.1.html>

Team, P., 2021. Todo lo que debes saber de Cisco Packet Tracer. [Online] Ambitbst.com. Recuperado de: <https://www.ambit-bst.com/blog/todo-lo-que-debes-saber-de-cisco-packet-tracer>.