

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

URIEL EDUARDO TIBOCHA TIRANO

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

URIEL EDUARDO TIBOCHA TIRANO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 28 noviembre de 2021

AGRADECIMIENTOS

Agradecimiento primeramente a DIOS por permitirme culminar este programa académico, a mis seres queridos por apoyarme en cada dificultad que se me presento en el trascurso de este logro, a los docentes que estuvieron pendientes a cualquier inquietud que surgía en el desarrollo de las actividades, a mi familia quienes aportaron en no desfallecer y ser un ejemplo para ellos de superación personal.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO.....	5
GLOSARIO	10
RESUMEN	11
ABSTRACT	12
ESCENARIO	14
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.	16
Paso 1: Cablear la red como se muestra en la topología.	16
Paso 2: Configurar los parámetros básicos para cada dispositivo.....	16
Parte 2: Configurar la capa 2 de la red y el soporte de Host.....	22
Tarea 2.1: Habilite enlaces trunk 802.1Q.....	23
Tarea 2.2: Use VLAN 999 Como la VLAN native.....	24
Tarea 2.3: Use Rapid Spanning Tree (RSPT).	24
Tarea 2.4: Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch	25
Tarea 2.5: En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	25
Tarea 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.	26
Tarea 2.7: Verifique los servicios DHCP IPv4.....	27
Tarea 2.8: Verifique la conectividad de la LAN local.....	28
Parte 3: Configurar los protocolos de enrutamiento	30
Tarea 3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2),	

configure single-area OSPFv2 en area 0.....	31
Tarea 3.2: En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.....	32
Tarea 3.3: En R2 en la “Red ISP”, configure MP-BGP.....	34
Tarea 3.4: En R1 en la “Red ISP”, configure MP-BGP.....	35
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).....	36
Tarea 4.1: En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.....	38
Tarea 4.2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.....	39
Tarea 4.3: En D1 configure HSRPv2.....	40
Parte 5: Seguridad.....	42
Tarea 5.1: En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.....	43
Tarea 5.2: En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.....	43
Tarea 5.3: En todos los dispositivos (excepto R2), habilite AAA.....	43
Tarea 5.4: En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.....	43
Tarea 5.5: En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.....	44
Tarea 5.6: Verifique el servicio AAA en todos los dispositivos (except R2).....	44
Parte 6: Configure las funciones de Administración de Red.....	47
Tarea 6.1: En todos los dispositivos, configure el reloj local a la hora UTC actual.....	47
Tarea 6.2: Configure R2 como un NTP maestro.....	48
Tarea 6.3: Configure NTP en R1, R3, D1, D2, y A1.....	48

Tarea 6.4: Configure Syslog en todos los dispositivos excepto R2	50
Tarea 6.5: Configure SNMPv2c en todos los dispositivos excepto R2	51
CONCLUSIONES	53
BIBLIOGRAFÍA	54

LISTA DE TABLAS

Tabla 1:Tabla de direccionamiento	15
Tabla 2: Tareas de configuración parte 2.....	22
Tabla 3: Tareas de configuración parte 3.....	30
Tabla 4: Tabla tareas parte 4 Configurar la Redundancia del Primer Salto (First Hop Redundancy)	36
Tabla 5: Tabla tareas parte 5 seguridad	42
Tabla 6: Tareas parte 6 Configure las funciones de Administración de Red	47

LISTA DE FIGURAS

Ilustración 1: Escenario 1.....	14
Ilustración 2: Topología GNS3.....	15
Ilustración 3:Conexión de Topología.....	16
Ilustración 4:Asignación IP PC1.....	21
Ilustración 5: asignación IP PC4.....	21
Ilustración 6: Direccionamiento IP PC2.....	27
Ilustración 7: Direccionamiento IP PC3.....	27
Ilustración 8: pings PC1.....	28
Ilustración 9:pings PC2.....	28
Ilustración 10:pings PC3.....	29
Ilustración 11:pings PC 4.....	29
Ilustración 12:show ip sla summary.....	38
Ilustración 13: show ip sla summary D2.....	39
Ilustración 14: show standby brief D1.....	41
Ilustración 15: Autenticación AAA R1 GNS3v.....	44
Ilustración 16: Autenticación AAA R3 GNS3.....	45
Ilustración 17: Autenticación AAA D1 GNS3.....	45
Ilustración 18: Autenticación AAA D2 GNS3.....	46
Ilustración 19: Autenticación AAA A1 GNS3.....	46
Ilustración 20: show NTP status R2.....	48
Ilustración 21:show NTP associations R1.....	49
Ilustración 22:show NTP associations R3.....	49
Ilustración 23: show NTP associations D1.....	49
Ilustración 24: show NTP associations A1.....	50
Ilustración 25: show NTP associations D2.....	50

GLOSARIO

GNS3 (Graphic Network Simulation): es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, están vinculadas aplicaciones como Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios, imágenes IOS de Cisco Systems, Dynagen, un front-end basado en texto para Dynamips, entre otros, según (universidad complutense, s.f.)

Conmutación: es la acción de establecer una vía, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión, según (ecured.com, s.f.)

Enrutamiento: es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta, mediante dispositivos de red que tienen dos o más interfaces para conectarse a diferentes redes. Antes de llegar a su destino, un paquete generalmente tiene que pasar a través de varias redes y los enrutadores son los dispositivos que reenviarán el paquete de una red a otra, según (tecnoseguro.com, s.f.)

Networking: es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos, mediante dispositivos de computación conectados en nodos que pasan los datos entre sí a lo largo de las conexiones de datos, ya sea por cable o medios inalámbricos, según (computerweekly.com, s.f.)

Electrónica: Emplea sistemas cuyo funcionamiento se basa en la conducción y el control del flujo de los electrones u otras partículas cargadas eléctricamente

RESUMEN

Este documento es una prueba de habilidades prácticas para el diplomado de profundización CCNP, como opción de grado al título como Ingeniero en Telecomunicaciones de la Universidad Nacional Abierta y a Distancia UNAD, se realiza la configuración e identifican problemas con aspectos de conmutación y enrutamiento, mediante el uso de comandos IOS, en los dispositivos configurados en el software de simulación GNS3.

Este trabajo está comprendido por seis partes, las cuales tienen el paso a paso de cada configuración llevada a cabo, propendiendo a que se tenga accesibilidad de un extremo a otro en cada uno de los dispositivos, en cuanto a su direccionamiento de interfaces, configuración de switch en capa 2, habilitación de protocolos spanning-tree, etherchannels, DHCP, OSPFv2, OSPFv3, BGP, se dispone HSRPv2 para proveer redundancia.

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

ABSTRACT

This document is a test of practical skills for the CCNP deepening diploma, as a degree option to the degree as Telecommunications Engineer from the National Open and Distance University UNAD, the configuration is carried out and problems with switching and routing aspects are identified, through the use of IOS commands, in the devices configured in the GNS3 simulation software.

This work is comprised of six parts, which have the step by step of each configuration carried out, tending to have accessibility from one end to the other in each of the devices, in terms of its addressing of interfaces, configuration of Layer 2 switch, enabling spanning-tree protocols, etherchannels, DHCP, OSPFv2, OSPFv3, BGP, HSRPv2 is available to provide redundancy.

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

INTRODUCCIÓN

La elaboración de este documento es el resultado como prueba de habilidades prácticas para el diplomado de profundización CCNP, como opción de grado al título como Ingeniero en Telecomunicaciones de la Universidad Nacional Abierta y a Distancia UNAD, el cual consolida la configuración de un escenario en una topología de red de una compañía, aplicando los conocimientos adquiridos en el transcurso de este diplomado.

Se busca profundizar y afianzar conceptos de conmutación y enrutamiento que se aprendieron en el desarrollo de cada actividad, logrando adquirir habilidades en la configuración y desarrollo de un escenario con diferentes dispositivos de red como routers, switch y computadores, así como sus puertos, interfaces que cada dispositivo contiene.

En el desarrollo de este trabajo con opción de grado se construye una red, primeramente, configurando parámetros básicos en cada dispositivo y direccionamiento de sus interfaces, se configuran los switches en capa 2, habilitando protocolo spanning-tree, etherchannels, DHCP, así mismo se configuran protocolos de OSPFv2 y OSPFv3, BGP, se dispone HSRPv2 para proveer redundancia.

En el tema de seguridad de dispositivos se configura mecanismos como algoritmo de encriptación SCRYPT, AAA, especificaciones de servidor RADIUS, de la misma forma funciones de administración de red como NTP, SYSLOG, SNMPv2. Mediante los comandos "show y comandos ping" se verificará la correcta programación de los diferentes dispositivos como los router y switches y los 4 PC de la topología.

ESCENARIO

Ilustración 1: Escenario 1

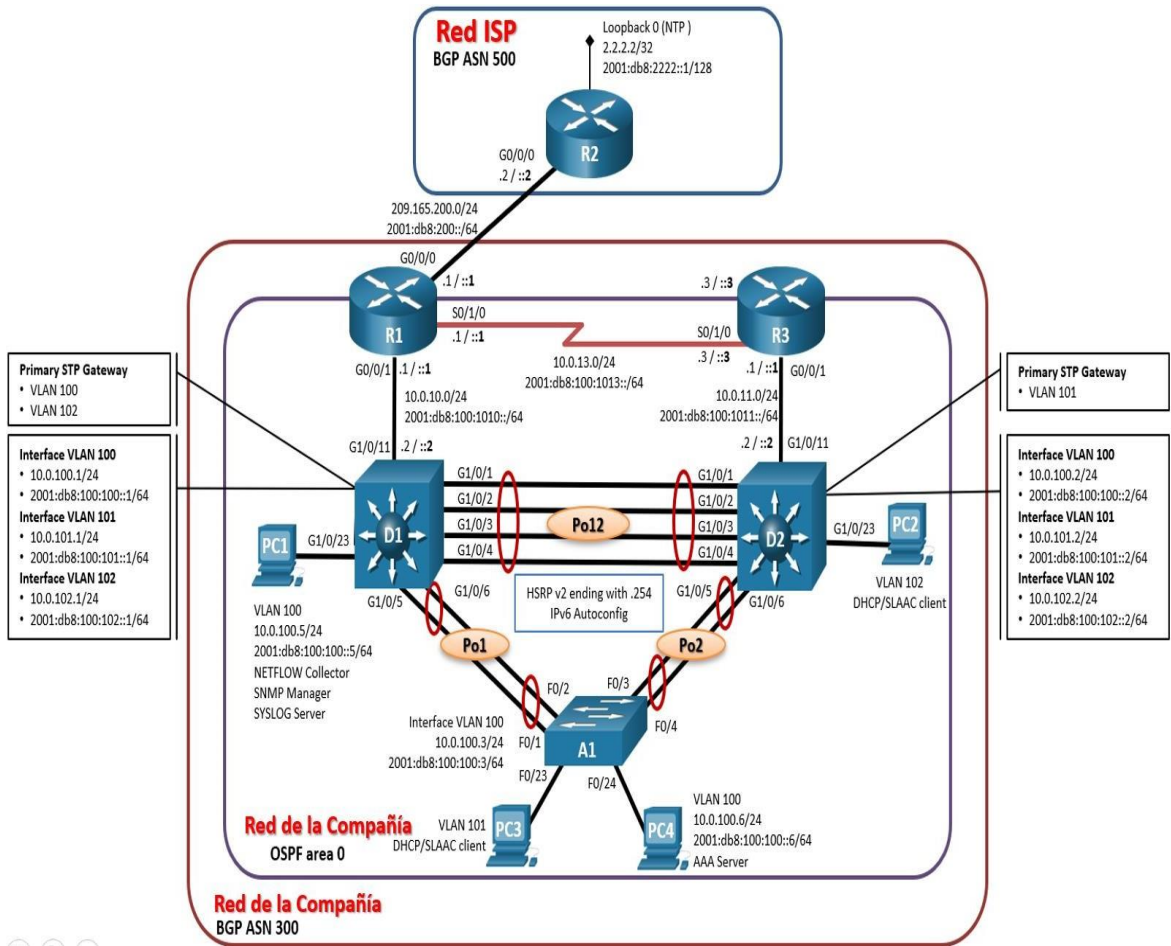
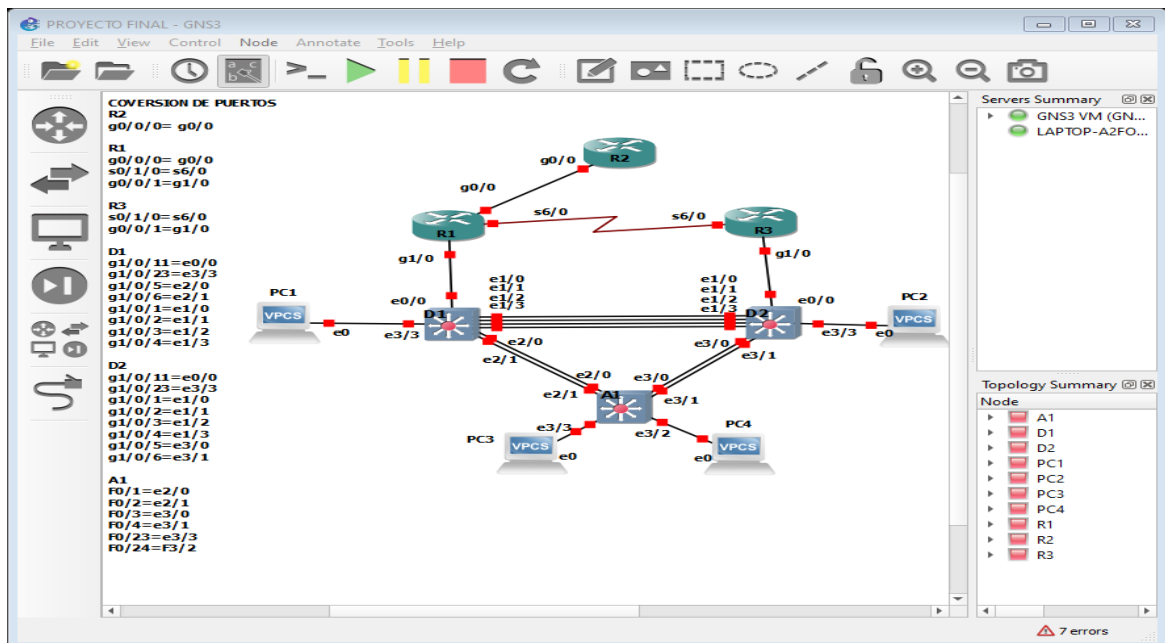


Tabla 1: Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S6/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S6/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E0/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E0/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Ilustración 2: Topología GNS3



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.

Ilustración 3: Conexión de Topología

CONVERSION DE PUERTOS

R2
g0/0/0= g0/0

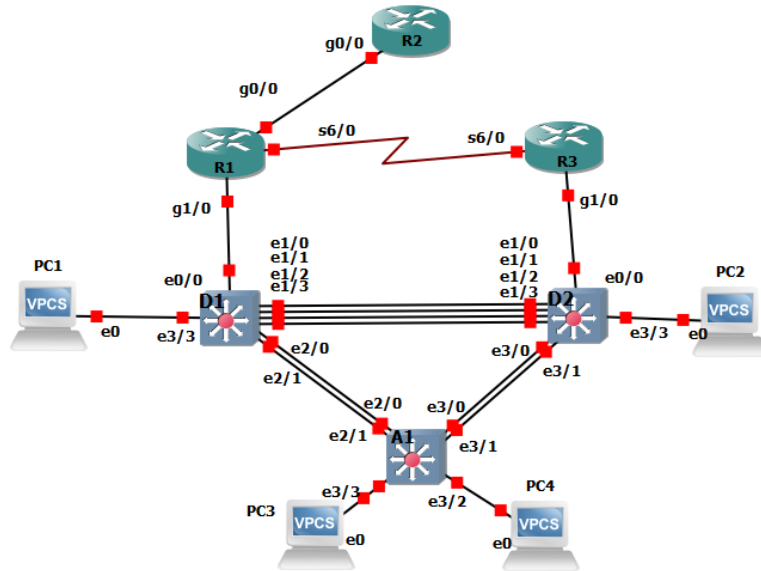
R1
g0/0/0= g0/0
s0/1/0=s6/0
g0/0/1=g1/0

R3
s0/1/0=s6/0
g0/0/1=g1/0

D1
g1/0/11=e0/0
g1/0/23=e3/3
g1/0/5=e2/0
g1/0/6=e2/1
g1/0/1=e1/0
g1/0/2=e1/1
g1/0/3=e1/2
g1/0/4=e1/3

D2
g1/0/11=e0/0
g1/0/23=e3/3
g1/0/1=e1/0
g1/0/2=e1/1
g1/0/3=e1/2
g1/0/4=e1/3
g1/0/5=e3/0
g1/0/6=e3/1

A1
f0/1=e2/0



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:

Se adjunta código y pantallazos con veracidad del código.

Router R1

```

Router>enable //Ingreso a modo privilegiado
Router#configure terminal //Ingreso modo configuración
Router(config)#
Router(config)#hostname R1 //Asigno nombre al router
R1(config)#ipv6 unicast-routing //Habilita routing IPv6
R1(config)#no ip domain lookup //Desactivar la búsqueda DNS
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0 //Ingreso configuración de línea de la consola
R1(config-line)#exec-timeout 0 0 //Desconexión por inactividad en una sesión
    
```

```

R1(config-line)#logging synchronous //sincroniza msj con comandos en prompt del SO
R1(config-line) #exit
R1(config)#interface g0/0 //configuración de interfaz g0/0
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 //se activa la interfaz
R1(config-if)#exit
R1(config)#interface g1/0 //configuración de interfaz g1/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown //se activa la interfaz
R1(config-if)#exit
R1(config)#interface s6/0 //configuración de interfaz s6/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0 //asignación de ipv4 y ipv6
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 //se activa la interfaz
R1(config-if)#exit
R1(config)#
R1# copy running-config startup-config //copiar la configuración en ejecución al archivo de
configuración de inicio

Router R2
Router>
Router>enable //Ingreso a modo privilegiado
Router#conf ter //Ingreso modo configuración
Router(config)#hostname R2 //Asigno nombre al router
R2(config)#ipv6 unicast-routing //Habilita routing IPv6 en el router
R2(config)#no ip domain lookup //Desactivar la búsqueda DNS
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 # banner
R2(config)#line con 0 //Ingreso configuración de línea de la consola
R2(config-line)#exec-timeout 0 0 //Desconexión por inactividad en una sesión
R2(config-line)#logging synchronous //sincroniza msj con comandos en prompt del SO
R2(config-line)#exit //salida modo line
R2(config)#interface g0/0 //configuración de interfaz g0/0,
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 //se activa la interfaz
R2(config-if)#exit
R2(config)#interface Loopback 0 //configuración dirección de loopback
R2(config-if)#
R2(config-if)#ip address 2.2.2.2 255.255.255.255 //dirección de loopback 0
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 //se activa la interfaz
R2(config-if)#exit
R2# copy running-config startup-config //copiar la configuración en ejecución al archivo de
configuración de inicio

```

```

Router R3
Router>enable //Ingreso a modo privilegiado
Router#conf terminal //Ingreso modo configuración
Router(config)#hostname R3 //Asigno nombre al router
R3(config)#ipv6 unicast-routing //Habilita el routing IPv6 en el router
R3(config)#no ip domain lookup //Desactivar la búsqueda DNS
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0 //Ingresar al modo de configuración
R3(config-line)#exec-timeout 0 0 //Desconexión por inactividad en una sesión
R3(config-line)#logging synchronous //sincroniza msj con comandos en prompt del SO
R3(config-line)#exit //salida modo line
R3(config)#interface g1/0 //configuración de interfaz G1/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0 //asignacion de ip
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 //se activa la interfaz
R3(config-if)#exit
R3(config)#interface s6/0 //configuración de interfaz s6/0
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 //se activa la interfaz
R3(config-if)#
R3(config-if)#exit
R3# copy running-config startup-config //copiar la configuración en ejecución al archivo de
configuración de inicio

Switch D1
Switch>enable //Ingreso a modo privilegiado
Switch#conf terminal //Ingreso modo configuración
Switch(config)#hostname D1 //Asigno nombre al switch
D1(config)#ip routing //habilita el protocolo de Internet
D1(config)#ipv6 unicast-routing //Habilita el routing IPv6 en el router
D1(config)#no ip domain lookup //Desactivar la búsqueda DNS
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 # //banner
D1(config)#line con 0 //Ingreso configuración de línea de la consola
D1(config-line)#exec-timeout 0 0 //Desconexión por inactividad en una sesión
D1(config-line)#logging synchronous //sincroniza msj con comandos en prompt del SO
D1(config-line)#exit
D1(config)#vlan 100 //configuración vlan 100
D1(config-vlan)#name Management //nombre de vlan 100
D1(config-vlan)#exit
D1(config)#vlan 101 //configuración vlan 101
D1(config-vlan)#name UserGroupA //nombre de vlan UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102 //configuración vlan 102
D1(config-vlan)#name UserGroupB //nombre de vlan UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999 //configuración vlan 999
D1(config-vlan)#name NATIVE //nombre de vlan NATIVE
D1(config-vlan)#exit
D1(config)#interface e0/0 //configuración interfaz e0/0
D1(config-if)#no switchport //activación de puertos
D1(config-if)#ip address 10.0.10.2 255.255.255.0 //asignación de ipv4

```

```

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 //se activa la interfaz
D1(config-if)#exit
D1(config)#interface vlan 100 //configuración vlan 100
D1(config-if)#ip address 10.0.100.1 255.255.255.0 //asignación de ipv4
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64 //asignación de dirección ipv6
D1(config-if)#no shutdown //se activa la interfaz
D1(config-if)#exit
D1(config)#interface vlan 101 //configuración interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0 //asignación de ipv4
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64 //asignación de dirección ipv6
D1(config-if)#no shutdown //se activa la interfaz
D1(config-if)#exit
D1(config)#interface vlan 102 //configuración interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0 //asignación de ipv4
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64 //asignación de dirección ipv6
D1(config-if)#no shutdown //se activa la interfaz
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 //configuración DHCP pool vlan 101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0 //direccionamiento de red
D1(dhcp-config)#default-router 10.0.101.254 //direccionamiento por default router
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102 //configuración DHCP pool vlan 102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0 //direccionamiento de red
D1(dhcp-config)#default-router 10.0.102.254 //direccionamiento por default router
D1(dhcp-config)#exit
D1(config)#interface range g2/0-3,g3/0-2 //selección de rango de interfaz
D1(config-if-range)#shutdown //desactivación selección rango
D1(config-if-range)#exit
D1(config)#

Switch D2
Switch>enable //Ingreso a modo privilegiado
Switch#conf ter //Ingreso modo configuración
Switch(config)#hostname D2 //Asigno nombre al switch
D2(config)#ip routing //habilita el protocolo de Internet
D2(config)#ipv6 unicast-routing //Habilita el routing IPv6 en el router
D2(config)#no ip domain lookup //Desactivar la búsqueda DNS
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0 //Ingresar al modo de configuración de línea de la consola
D2(config-line)#exec-timeout 0 0 //Desconexión por inactividad
D2(config-line)#logging synchronous //sincroniza msj con comandos en prompt
del SO D2(config-line)#exit
D2(config)#vlan 100 //configuración vlan 100
D2(config-vlan)#name Management //nombre de vlan 100

```

```

D2(config-vlan)#exit
D2(config)#vlan 101 //configuración vlan 101
D2(config-vlan)#name UserGroupA //nombre de vlan UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102 //configuración vlan 102
D2(config-vlan)#name UserGroupB // de vlan UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999 //configuración vlan 999
D2(config-vlan)#name NATIVE //nombre de vlan NATIVE
D2(config-vlan)#exit
D2(config)#interface e0/0 //selección de interfaz
D2(config-if)#no switchport //activación interfaz
D2(config-if)#ip address 10.0.11.2 255.255.255.0 // asignación de ipv4
D2(config-if)#ipv6 address fe80::d1:1 link-local // dirección ipv6
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64 //se activa la interfaz
D2(config-if)#no shutdown //se activa la interfaz
D2(config-if)#exit
D2(config)#interface vlan 100 //configuración 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 // asignación de dirección ipv6
D2(config-if)#no shutdown //se activa la interfaz
D2(config-if)#exit
D2(config)#interface vlan 101 //configuración interface vlan 101
D2(config-if)#
D2(config-if)#ip address 10.0.101.2 255.255.255.0 // asignación de ipv4
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64 // asignación de dirección ipv6
D2(config-if)#no shutdown // se activa la interfaz
D2(config-if)#exit
D2(config)#interface vlan 102 //configuración vlan interface 101
D2(config-if)#
D2(config-if)#ip address 10.0.102.2 255.255.255.0 // asignación de ipv4
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64 // asignación de dirección ipv6
D2(config-if)#no shutdown //se activa la interfaz
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 //configuración DHCP pool vlan 101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0 //direccionamiento de red
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102 //configuration DHCP pool vlan 102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0 direccionamiento de red
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range e0/0-3, e1/0-3 //selección de rango de interfaz
D2(config-if-range)#shutdown //desactivación selección puertos
D2(config-if-range)#
D2(config-if-range)#exit //Salida Rango de interfaces

```

```

D2(config)#
D2#copy running-config startup-config //copiar la configuración en ejecución al
                                        //archivo de configuración de inicio

Switch A1
Switch>enable //Ingreso a modo privilegiado
Switch#conf ter //Ingreso modo configuración
Switch(config)#hostname A1 //Asigno nombre al switch
A1(config)#no ip domain lookup //Desactivar la búsqueda DNS
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0 //Ingresar al modo de configuración de línea de la consola
A1(config-line)#exec-timeout 0 0 //Desconexión por inactividad
A1(config-line)#logging synchronous //sincroniza msj con comandos en prompt del SO
A1(config-line)#exit //Salida line
A1(config)#vlan 100 //configuracion vlan 100
A1(config-vlan)#name Management //nombre de vlan
A1(config-vlan)#exit
A1(config)#vlan 101 //configuración vlan 101
A1(config-vlan)#name UserGroupA //nombre de vlan
A1(config-vlan)#exit
A1(config)#vlan 102 //configuración vlan 102
A1(config-vlan)#name UserGroupB //nombre de vlan UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999 //configuración vlan native
A1(config-vlan)#name NATIVE //nombre de vlan native
A1(config-vlan)#exit
A1(config)#interface vlan 100 //configuración vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0 //asignación de ipv4
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64 // asignación de dirección ipv6
A1(config-if)#no shutdown //se activa la interfaz
A1(config-if)#exit
A1#copy running-config startup-config //copiar la configuración en ejecución al
                                        //archivo de configuración de inicio

```

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.

Ilustración 4:Asignación IP PC1

```

PC1> sh

```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC1	10.0.100.5/24	10.0.100.254	00:50:79:66:68:00	20044	127.0.0.1:20045
	fe80::250:79ff:fe66:6800/64				
	2001:db8:100:100::5/64				

Ilustración 5: asignación IP PC4

```

PC4> sh

```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC4	10.0.100.6/24	10.0.100.254	00:50:79:66:68:03	20048	127.0.0.1:20049
	fe80::250:79ff:fe66:6803/64				
	2001:db8:100:100::6/64				

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.

Las tareas de configuración son las siguientes:

Tabla 2: Tareas de configuración parte 2

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 <p>PC1: 10.0.100.5</p>
-----	---	---

Tarea 2.1: Habilite enlaces trunk 802.1Q.

D1 and D2

D1>enable

D1#conf term //ingreso configuración global

D1(config)#

D1(config)#interface range e1/0-3 //configuración modo trunk interfaz D1

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

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

D1(config-if-range)#switchport trunk native vlan 999

D1(config-if-range)#switchport trunk allowed vlan 100,101,102

D1(config-if-range)#

D1(config-if-range)#end

D2>enable

D2#conf term //ingreso configuración global

D2(config)#

D2(config)#interface range e1/0-3 //configuración modo trunk interfaz D2

D2(config-if-range)#switchport trunk encapsulation dot1q

D2(config-if-range)#switch mode trunk

D2(config-if-range)#switchport trunk native vlan 999

D2(config-if-range)#switchport trunk allowed vlan 100,101,102

D1 and A1

D1>enable

D1#conf term

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

D1(config)#

D1(config)#interface range e2/0-1 //configuración modo trunk interfaz

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

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

```
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#switchport trunk allowed vlan 100,101,102
D1(config-if-range)#
D1(config-if-range)#end
```

```
A1(config)#interface range e2/0-1 //configuración modo trunk interfaz
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#switchport trunk allowed vlan 100,101,102
A1(config-if-range)#end
```

```
D2 and A1
D2>enable
D2#conf term
D2(config)#
D2(config)#interface range e3/0-1 //configuración modo trunk interfaz
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switch mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#switchport trunk allowed vlan 100,101,102
```

```
A1(config)#interface range e3/0-1 //configuración modo trunk interfaz
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#switchport trunk allowed vlan 100,101,102
A1(config-if-range)#end
```

Tarea 2.2: Use VLAN 999 Como la VLAN native.

```
D1(config-if-range)#switchport trunk native vlan 999 // config. vlan 999 native
D2(config-if-range)#switchport trunk native vlan 999 // config. vlan 999 native
A1(config-if-range)#switchport trunk native vlan 999 // config. vlan 999 native
```

Tarea 2.3: Use Rapid Spanning Tree (RSPT).

```
D1#enable
D1#conf ter //ingreso configuración global
D1(config)#interface range e1/0-3 //selección de interfaz
D1(config-if-range)#spanning-tree mode pvst //configuración RSPT
D1(config)#interface range e2/0-1 //selección de interfaz
D1(config-if-range)#spanning-tree mode pvst // configuración RSPT
D1(config)#interface range e0/0 //selección de interfaz
D1(config-if-range)#spanning-tree mode pvst // configuración RSPT D1(config)#interface range
e3/3 //selección de interfaz
D1(config-if-range)#spanning-tree mode pvst // configuración RSPT
D1(config)#
```

```
D2#enable
D2#conf ter //ingreso configuración global
D2 (config)#interface range e1/0-3 //selección de interfaz
D2 (config-if-range)#spanning-tree mode pvst //configuración RSPT
```

```

D2 (config)#interface range e3/0-1 //selección de interfaz
D2 (config-if-range)#spanning-tree mode pvst //configuración RSPT
D2 (config)#interface range e0/0 //selección de interfaz
D2 (config-if-range)#spanning-tree mode pvst //configuración RSPT
D2 (config)#interface range e3/3 //selección de interfaz
D2 (config-if-range)#spanning-tree mode pvst //configuración RSPT

A1#enable
A1#conf ter //ingreso configuración global
A1 (config)#interface range e2/0-1 //selección de interfaz
A1 (config-if-range)#spanning-tree mode pvst //configuración RSPT
A1 (config)#interface range e3/0-3 //selección de interfaz
A1 (config-if-range)#spanning-tree mode pvst //configuración RSPT

```

Tarea 2.4: Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch

Se configura D1 con spanning-tree las vlan 100 y 102 como raíz primaria y 101 como raíz secundaria, así mismo el D2 con las vlan 100, 102 como raíz secundaria y 101 como raíz primaria

```

D1#conf termin //configuración global
D1(config)#spanning-tree vlan 100 root primary // configuración D1 raíz primario

D1(config)#spanning-tree vlan 101 root secondary
D1(config)#spanning-tree vlan 102 root primary

D2#conf ter
D2(config)# //configuración global
D2(config)#spanning-tree vlan 100 root secondary // configuración D2 raíz secundario
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 102 root secondary

```

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

Se configura port channel entre cada dispositivo

D1 a D2 – Port channel 12

```

D1>enable
D1#confi ter //ingreso configuración global
D1(config)#interface range e1/0-3 //selección de rango interfaz
D1(config-if-range)#CHANNEL-GROUP 12 mode active //asignación port channel
D2>enable
D2#confi ter //ingreso configuración global
D2 (config)#interface range e1/0-3 //selección de rango interfaz
D2(config-if-range)#CHANNEL-GROUP 12 mode active //asignación port channel

```

D1 a A1 – Port channel 1

```

D1#CONF TERM
D1(config)# //ingreso configuración global
D1(config)#interface range e2/0-1 //selección de rango interfaz
D1(config-if-range)#CHANNEL-GROUP 1 mode active //asignación port channel
A1#conf term

```

```

A1 (config)# //ingreso configuración global
A1(config)#interface range e2/0-1 //selección de rango interfaz
A1 (config-if-range)#CHANNEL-GROUP 1 mode active //asignación port channel

```

D2 a A1 – Port channel 2

```

D2#conf term
D2 (config)# //ingreso configuración global
D2 (config)#interface range e3/0-1 //selección de rango interfaz
D2 (config-if-range)#CHANNEL-GROUP 2 mode active //asignación port channel
A1#conf terminal //ingreso configuración global
A1 (config)#
A1(config)#interface range e3/0-1 //selection de Rango interfaz
A1 (config-if-range)#CHANNEL-GROUP 2 mode active //asignación port channel

```

Tarea 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.

Acceso pc 1

```

D1#configure terminal //acceso modo global
D1(config)#Interface e3/3 //selección interfaz
D1(config-if)#switchport mode access //configuración modo access vlan 100
D1(config-if)#switch access vlan 100

```

Acceso pc2

```

D2# configure terminal //acceso modo global
D2(config)#interface e3/3 //selección interfaz
D2(config-if)#switchport mode access //configuración modo access vlan 102
D2(config-if)#switch acces vlan 102

```

Acceso a pc3

```

A1#configure terminal //acceso modo global
A1(config)#interfaz e3/3 //selección interfaz
A1(config-if)#switchport mode access //configuración modo access vlan 101
A1(config-if)#switch access vlan 101

```

Acceso a pc4

```

A1#configure terminal //acceso modo global
A1(config)#interface e3/2 //selección interfaz
A1(config-if)#switchport mode access //configuración modo access vlan 101
A1(config-if)#switch access vlan 100

```

Tarea 2.7: Verifique los servicios DHCP IPv4

Ilustración 6: Direccionamiento IP PC2

The screenshot displays the GNS3 network simulator interface. On the left, a list of port conversion rules is visible under the heading "CONVERSION DE PUERTOS". The main area shows a network topology with three routers (R1, R2, R3), three switches (D1, D2, D3), and four PCs (PC1, PC2, PC3, PC4). A terminal window for PC2 is open, showing the following commands and output:

```
PC2> ip dhcp
DORAORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> ora
```

The Windows taskbar at the bottom shows the time as 06:11 p.m. on 20/11/2021.

Ilustración 7: Direccionamiento IP PC3

This screenshot shows the same GNS3 network simulator interface as the previous one. The terminal window for PC3 is now active, displaying the following output:

```
welcome to Virtual PC Simulator, version 0.8.2
dedicated to Delling.
build time: Aug 23 2021 11:15:00
copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
all rights reserved.

PCS is free software, distributed under the terms of the "BSD" licence.
source code and license can be found at vpcs.sf.net,
or more information, please visit wiki.freecode.com.cn.

press '?' to get help.

xecuting the startup file

C3>
C3> ip dhcp
DORAORA IP 10.0.101.210/24 GW 10.0.101.254
C3>
```

The Windows taskbar at the bottom shows the time as 06:24 p.m. on 20/11/2021.

Tarea 2.8: Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC4: 10.0.100.6

Ilustración 8: pings PC1

The screenshot shows the GNS3 interface with a network topology and a terminal window for PC1. The topology includes three routers (R1, R2, R3) and four PCs (PC1, PC2, PC3, PC4). The terminal window displays the following output:

```
PC1: show ip
IP/MASK : 10.0.100.5/24
GATEWAY : 10.0.100.254
HS :
AC : 00:50:79:66:68:00
PORT : 20044
HOST:PORT : 127.0.0.1:20045
RTU : 1500

PC1> ping 10.0.100.1
4 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.359 ms
4 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.391 ms
4 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.413 ms
4 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.367 ms
4 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.416 ms

PC1> ping 10.0.100.2
4 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.427 ms
4 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.578 ms
4 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.718 ms
4 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.656 ms
4 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.623 ms

PC1> ping 10.0.100.6
4 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.563 ms
4 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=0.773 ms
4 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.684 ms
4 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.813 ms
4 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.584 ms

PC1>
```

PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

D2: 10.0.102.2

Ilustración 9: pings PC2

The screenshot shows the GNS3 interface with the same network topology as in the previous image. The terminal window for PC2 displays the following output:

```
PC2: show ip
NAME : PC2[1]
IP/MASK : 10.0.102.110/24
GATEWAY : 10.0.102.254
DNS :
DHCP SERVER : 10.0.102.1
DHCP LEASE : 85322, 86400/43200/75600
MAC : 00:50:79:66:68:01
PORT : 20046
HOST:PORT : 127.0.0.1:20047
RTU : 1500

PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.513 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.640 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.678 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.728 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.740 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.269 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.357 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.342 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.361 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.296 ms

PC2>
```

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

Ilustración 10:pings PC3

The screenshot shows a GNS3 network simulation. On the left, a list of configurations for various devices (R1, R2, R3, D1, D2, A1) is visible. The central part of the image shows a network diagram with three routers (R1, R2, R3) and several PCs (PC1, PC2, PC3, PC4). PC3 is highlighted in blue. On the right, a terminal window for PC3 displays the following output:

```

host (10.0.101.2) not reachable
PC3> ping 10.0.101.3
host (10.0.101.3) not reachable
PC3> ping 10.0.100.3
host (10.0.101.254) not reachable
PC3> ip dhcp
DORA IP 10.0.101.110/24 GW 10.0.101.254
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.420 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.517 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=0.626 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=1.019 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.595 ms
PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.531 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.844 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=0.845 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.777 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.774 ms
  
```

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

Ilustración 11:pings PC 4

The screenshot shows the same GNS3 network simulation. The terminal window for PC4 displays the following output:

```

IP/PSOCK : 10.0.100.0/24
GATEWAY : 10.0.100.254
DNS :
MAC : 00:50:79:66:68:03
LPORT : 20050
RHOST:PORT : 127.0.0.1:20051
RTU : 1500
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.386 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.619 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.588 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.573 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.600 ms
PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.562 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.166 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.414 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.852 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.973 ms
PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.442 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.684 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.859 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.833 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.742 ms
  
```

Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Tabla 3: Tareas de configuración parte 3

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 la ruta 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 redes directamente 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 la ruta 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

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

Se configura OSPFv2 usando OSPF Process ID 4 y asigne los router-IDs

```
R1: 0.0.4.1
R1#conf ter //configuración global
R1(config)#router ospf 4 // configuración OSPF Process ID 4
R1(config-router)#router-id 0.0.4.1 //asignación de ID
```

```
R3: 0.0.4.3
R3#conf ter //configuración global
R3(config)#
R3(config)#router ospf 4 // configuración OSPF Process ID 4
R3(config-router)#router-id 0.0.4.3 //asignación de ID
```

```
D1: 0.0.4.131
D1#conf ter //configuración global
D1(config)#
D1(config)#router ospf 4 // configuración OSPF Process ID 4
D1(config-router)#router-id 0.0.4.131 //asignación de ID
```

```
D2: 0.0.4.132
D2(config)# //configuración global
D2(config)#router ospf 4 //configuración OSPF Process ID 4
D2(config-router)#router-id 0.0.4.132 //asignación de ID
```

En R1, R3, D1, y D2, se anuncian todas las redes directamente conectadas y también las VLANs en Area 0.

```
R1 //anuncio de redes R1 en area 0
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)#passive-interface g1/0 //Evita actualizaciones innecesarias
```

```
R3 //anuncio de redes R3 en area 0
R2(config-router)#network 10.0.11.0 0.0.0.255 area 0
R2(config-router)#network 10.0.13.0 0.0.0.255 area 0
R2(config-router)#passive-interface g1/0 //Evita actualizaciones innecesarias
```

```
D1 //anuncio de redes D1 en area 0
D1(config-router)#do show ip route connected
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
```

```
D2 //anuncio de redes D2 en area 0
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)#network 10.0.102.0 0.0.0.255 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.

```
R1(config)#ipv6 router ospf 4 // Ingresa al router ospf 6.
R1(config-rtr)#router-id 0.0.4.1 //Asignación id 0.0.4.1.
R1(config-rtr)#default-information originate //asignación ruta predeterminada
```

Se deshabilitan las publicaciones OSPFv2 en D1 y D2 exceptuando en la interfaz e0/0

D1: todas las interfaces excepto e0/0

```
D1(config-router)#passive-interface e1/0
D1(config-router)#passive-interface e1/1
D1(config-router)#passive-interface e1/2
D1(config-router)#passive-interface e1/3
D1(config-router)#passive-interface e2/0
D1(config-router)#passive-interface e2/1
D1(config-router)#passive-interface e3/3
```

```
D2(config-router)#passive-interface e1/0 //deshabilitar publicaciones OSPFv2 en D1
D2(config-router)#passive-interface e1/1
D2(config-router)#passive-interface e1/2
D2(config-router)#passive-interface e1/3
D2(config-router)#passive-interface e3/0
D2(config-router)#passive-interface e3/1
D2(config-router)#passive-interface e3/3
```

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

Se configura OSPFv3 usando OSPF Process ID **6** y asigna los router-IDs, también se anuncian todas las redes y vlans directamente conectadas en área 0, en el R1 no se publica la red de R2, también se propaga una ruta por defecto provista por BGP

R1: 0.0.6.1

```
R1(config)#ipv6 router ospf 6 // Ingresa al router ospf 6.
R1(config-rtr)#router-id 0.0.6.1 // Asigna el id 0.0.6.1
R1(config-rtr)#default-information originate //ruta predeterminada
R1(config-rtr)#interface s6/0 //ingreso a interfaz
R1(config-if)#ipv6 ospf 6 area 0 //ingreso ipv6 ospf 6 area 0
R1(config-if)#exit //salida
R1(config)#interface gigabitEthernet 1/0 //ingreso interfaz G1/0
R1(config-if)#ipv6 ospf 6 area 0 //ingreso ipv6 ospf 6 area 0
R1(config-if)#exit //salida
```

R3: 0.0.6.3

```
R3(config)#ipv6 router ospf 6 // ingreso ipv6 ospf 6 area 0
R3(config-rtr)#router-id 0.0.6.3 // asignación id 0.0.6.3
R3(config-rtr)#interface s6/0 //ingreso interfaz s6/0
R3(config-if)#ipv6 ospf 6 area 0 //habilitar OSPFv3 en interfaz
R3(config-if)#exit //salida
R3(config)#interface gigabitEthernet 1/0 //ingreso interfaz G1/0
R3(config-if)#ipv6 ospf 6 area 0 //habilitar OSPFv3 en interfaz
```

```

D1: 0.0.6.131
D1(config)#ipv6 router ospf 6 //Habilita OSPFv3
D1(config-rtr)#router-id 0.0.6.131 //asignación id 0.0.6.131
D1(config-rtr)#interface e0/0 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D1(config)#interface vlan 100 //ingreso interfaz vlan 100
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D1(config-if)#interface vlan 101 //ingreso interfaz vlan 101
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D1(config-if)#interface vlan 102 //ingreso interfaz vlan 102
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D1(config-if)#interface e3/3 //ingreso interfaz e3/3
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e1/0 //no habilita ipv6 por falta ip
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e1/1 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e1/2 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e1/3 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e2/0 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D1(config-if)#interface e2/1 //ingreso interfaz
D1(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip

D2: 0.0.6.132
D2(config)#ipv6 router ospf 6 //Habilita OSPFv3
D2(config-rtr)#router-id 0.0.6.132 //asignación id 0.0.6.132
D2(config-rtr)#interface e0/0 //ingreso interfaz e0/0
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D2(config)#interface vlan 100 //ingreso interfaz vlan 100
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D2(config-if)#interface vlan 101 //ingreso interfaz vlan 101
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D2(config-if)#interface vlan 102 //ingreso interfaz vlan 102
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
D2(config-if)#interface e1/0 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e1/1 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e1/2 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz

```

```

% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e1/3 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e3/0 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e3/1 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip
D2(config-if)#interface e3/3 //ingreso interfaz
D2(config-if)#ipv6 ospf 6 area 0 //Habilita OSPFv3 en interfaz
% OSPFv3: IPV6 is not enabled on this interface //no Habilita ipv6 por falta ip

```

Se deshabilitan publicaciones de OSPFv3 en D1 Y D2 excepto en la interfaz e0/0

```

D1
D1(config)#ipv6 router ospf 6 //deshabilita publicaciones OSPFv3 en D1
D1(config-rtr)#passive-interface vlan 100
D1(config-rtr)#passive-interface vlan 101
D1(config-rtr)#passive-interface vlan 102

```

```

D2
D2(config)#ipv6 router ospf 6 //deshabilita publicaciones OSPFv3 en D2
D2(config-rtr)#passive-interface vlan 100
D2(config-rtr)#passive-interface vlan 101
D2(config-rtr)#passive-interface vlan 102

```

Tarea 3.3: En R2 en la "Red ISP", configure MP-BGP.

Se configuran dos rutas estáticas predeterminadas a través de la interfaz Loopback 0, para IPv4 y IPv6

```

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 //ruta estatica ipv4 con loopback 0
R2(config)#ipv6 route ::/0 loopback 0 //ruta estatica ipv6 con loopback 0

```

Se configura R2 en BGP ASN 500 y se usa el router-id 2.2.2.2.

```

R2(config)#router bgp 500 //Crea proceso BGP dentro del router
R2(config-router)#bgp router-id 2.2.2.2 //identificador de R2 en BGP

```

Se configura y habilita una relación de vecino IPv4 e IPv6 con R1 en ASN 300, también en IPv4 address family, se anuncian la red Loopback 0 IPv4 (/32) y la ruta por defecto (0.0.0.0/0), en IPv6 address family, se anuncia la red Loopback 0 IPv4 (/128), y la ruta por defecto (::/0).

```

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 //ruta por defecto ipv4
R2(config)#ipv6 route ::/0 loopback 0 //ruta por defecto ipv6
R2(config)#router bgp 500 //ruta de encaminamiento 500
R2(config-router)#bgp router-id 2.2.2.2 //identificador de R2 en BGP
R2(config-router)#neighbor 209.165.200.225 remote-as 300 //establecer vecinos de conexión
//ASN300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4 //configuración Familia ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate //relación router vecino

```

```

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 //anuncio red por BGP
R2(config-router-af)#network 0.0.0.0 // ruta estática
R2(config-router-af)#exit-address-family //salir de Familia ipv4
R2(config-router)#address-family ipv6 //configuración Familia IPV6
R2(config-router-af)#no neighbor 209.165.200.225 activate //negación ipv4 router1
R2(config-router-af)#neighbor 2001:db8:200::1 activate //relación router vecino
R2(config-router-af)#network 2001:db8:2222::/128 //configuración ipv6 router
R2(config-router-af)#network ::/0 // enrutamiento por defecto
R2(config-router-af)#exit-address-family //salir
R2(config-router)#

```

Tarea 3.4: En R1 en la "Red ISP", configure MP-BGP

Se configuran dos rutas resumen estáticas a la interfaz Null 0:

Una ruta resumen IPv4 para 10.0.0.0/8.

```
R1(config)#ip route 10.0.0.0 255.0.0.0 null0 //configuración ruta resumen IPV4
```

Una ruta resumen IPv6 para 2001:db8:100::/48.

```
R1(config)#ipv6 route 2001:db8:100::/48 null0 //configuración ruta resumen IPV6
```

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

```
R1(config-router)#bgp router-id 1.1.1.1 //identificador de R1 en BGP
```

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

```
//actualizar vecinos bgp IPV4 IPV6
```

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

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

En IPv4 address family:

```

R1(config-router)#address-family ipv4 //configura familia direcciones IPV4
R1(config-router-af)#neighbor 209.165.200.226 activate //Habilita relación vecino IPv4.
R1(config-router-af)#no neighbor 2001:db8:200::2 activate //Deshabilita relación vecino IPv6.
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0 //Anuncia la red 10.0.0.0/8
R1(config-router-af)#network 0.0.0.0
R1(config-router-af)#exit-address-family

```

En IPv6 address family:

```

R1(config-router)#address-family ipv6 //configura familia direcciones IPV6
R1(config-router-af)#no neighbor 209.165.200.226 activate //Deshabilita relación vecino IPv4
R1(config-router-af)#neighbor 2001:db8:200::2 activate //habilita relación vecino IPv6.
R1(config-router-af)#network 2001:db8:100::/48 //Anuncie la red 2001:db8:100::/48
R1(config-router-af)#network ::/0
R1(config-router-af)#exit-address-family

```

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

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

Las tareas de configuración son las siguientes:

Tabla 4: Tabla tareas parte 4 Configurar 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>Programa 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>Programa 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). <p>Rastree el objeto 6 y decremente en 60.</p>
-----	-------------------------	--

Tarea 4.1: En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.

Se crean dos IP SLA, usando el numero 4 para IPV4 y IPV6 para IPV6, estas IP SLAs probarán la disponibilidad de la interfaz R1 G1/0 cada 5 segundos y se programa la SLA para una implementación inmediata sintiempo de finalización

Use la SLA número 4 para IPv4.

```
D1(config)#ip sla 4 // definir # de IP SLA IPV4
D1(config-ip-sla)#icmp-echo 10.0.10.1 //tipo mensaje, IP, origen
D1(config-ip-sla-echo)#frequency 5 //frecuencia de monitoreo
D1(config-ip-sla-echo)#exit //salida ip-sla
```

Use la SLA número 6 para IPv6.

```
D1(config)#ip sla 6 // definir # de IP SLA IPV6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)#frequency 5 //frecuencia de monitoreo
D1(config-ip-sla-echo)#exit //salida ip-sla
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
```

Se crea una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6, los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de down y a up después de 10 segundos o de up a down después de 15 segundos

Se usa el número de rastreo 4 para la IP SLA 4.

```
D1(config)#track 4 ip sla 4 //definicion # rastreo ip sla 4
D1(config-track)#delay down 15 up 10 //down 15" y up 10"
D1(config-track)#exit
```

Se usa el número de rastreo 6 para la IP SLA 6.

```
D1(config)#track 6 ip sla 6 //definición # rastreo ip sla 4
D1(config-track)#delay down 15 up 10 //down 15" y up 10"
D1(config-track)#exit //salida
```

Ilustración 12:show ip sla summary

```
D1#show ip sla summary
PSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID          Type          Destination          Stats          Return Code          Last Run
-----
4           icmp-echo     10.0.10.1            -              Timeout              11 seconds ago
6           icmp-echo     2001:DB8:100:1010::1 -              Timeout              6 seconds ago

D1#
```

Tarea 4.2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0

Se crean IP SLAs en D2 usando la SLA número 4 para IPv4 y la SLA número 6 para IPv6, las cuales probaran la disponibilidad de la interfaz de R3 G1/0 cada 5 segundos, así mismo se programa la SLA para una implementación inmediata sin tiempo de finalización

```
D2(config)#ip sla 4 // definir # de IP SLA IPV4
D2(config-ip-sla)#icmp-echo 10.0.11.1 //tipo mensaje, IP, origen mensaje
D2(config-ip-sla-echo)#frequency 5 //frecuencia de monitoreo
D2(config-ip-sla-echo)#exit //salida
D2(config)#ip sla 6 // definir # de IP SLA IPV4
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 // mensaje, IP, origen IPV6
D2(config-ip-sla-echo)#frequency 5 //frecuencia de monitoreo
D2(config-ip-sla-echo)#exit //salida
D2(config)#ip sla schedule 4 life forever start-time now //Habilita IP SLA ahora y para siempre
D2(config)#ip sla schedule 6 life forever start-time now //Habilita IP SLA ahora y para siempre
```

Se crea una IP SLA objeto para la IP SLA 4 y una IP SLA 6, usando el número de rastreo 4 para la IP SLA 4 y el número de rastreo 6 para la SLA 6, estos 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(config)#track 4 ip sla 4 //Crea id objeto 4 y lo asocia con IP SLA4
D2(config-track)#delay down 15 up 10 //tiempo down y up
D2(config-track)#exit //salida
D2(config)#track 6 ip sla 6 //Crea id objeto 6 y lo socia con IP SLA6
D2(config-track)#delay down 15 up 10 //tiempo down y up
D2(config-track)#exit //salida
```

Ilustración 13: show ip sla summary D2



```
D2#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID          Type          Destination          Stats      Return Code    Last Run
-----
4           icmp-echo     10.0.11.1           -          Timeout        6 seconds ago

6           icmp-echo     2001:DB8:100:1011  -          Timeout        9 seconds ago

D2#
```

Tarea 4.3: En D1 configure HSRPv2.

Se cambia la prioridad a 150 de D1 siendo el router primario para las VLANs 100 y 102
Se configure HSRP version 2, y IPv4 HSRP grupo 104 para la VLAN 100

```
D1(config)# //configuración global
D1(config)#interface vlan 100 //interfaz vlan 100
D1(config-if)#standby version 2 //version 2
D1(config-if)#standby 104 ip 10.0.100.254 // Asigne la dirección IP virtual
D1(config-if)#standby 104 priority 150 //prioridad del grupo en 150
D1(config-if)#standby 104 preempt // Habilite la preferencia
D1(config-if)#standby 104 track 4 decrement 60 //Rastree el objeto 4 y
decremente en 60
D1(config-if)#exit //salida
```

Se configure IPv4 HSRP grupo 114 para la VLAN 101

```
D1(config)#interface vlan 101 //interfaz vlan 101
D1(config-if)#standby version 2 //version 2
D1(config-if)#standby 114 ip 10.0.101.254 // Asigne la dirección IP virtual
D1(config-if)#standby 114 preempt // Habilita la preferencia
D1(config-if)#standby 114 track 4 decrement 60 / //Rastree el objeto 4 y decremente 60
D1(config-if)#exit //salida
```

Se configure IPv4 HSRP grupo 124 para la VLAN 102

```
D1(config)#interface vlan 102 //interfaz vlan 102
D1(config-if)#standby version 2 //version 2
D1(config-if)#standby 124 ip 10.0.102.254 // Asigne la dirección IP virtual
D1(config-if)#standby 124 priority 150 //prioridad del grupo en 150
D1(config-if)#standby 104 preempt // Habilite la preferencia
D1(config-if)#standby 104 track 4 decrement 60 //Rastree el objeto 4 y decrementa 60
D1(config-if)#exit //salida
```

Se configure IPv6 HSRP grupo 106 para la VLAN 100

```
D1(config)#interface vlan 100 //interfaz vlan 100
D1(config-if)#standby version 2 //version 2
D1(config-if)#standby 106 ipv6 autoconfig // Asigne la dirección IP virtual
D1(config-if)#standby 106 priority 150 //prioridad del grupo en 150
D1(config-if)#standby 106 preempt // Habilite la preferencia
D1(config-if)#standby 106 track 4 decrement 60 //Rastree el objeto 4 y decrementa 60
D1(config-if)#exit
```

Configure IPv6 HSRP grupo 116 para la VLAN 101

```
D1(config)#interface vlan 101 //interfaz vlan 101
D1(config-if)#standby version 2 //version 2
D1(config-if)#standby 116 ipv6 autoconfig // Asigne la dirección IP virtual
D1(config-if)#standby 116 preempt // Habilita la preferencia
D1(config-if)#standby 116 track 4 decrement 60 //Rastree el objeto 4 y decrementa 60
D1(config-if)#exit
```

Configure IPv6 HSRP grupo 126 para la VLAN 102

```
D1(config)#interface vlan 102 //interfaz vlan 102
D1(config-if)#standby 126 ipv6 autoconfig // Asigne la dirección IP virtual
D1(config-if)#standby 126 priority 150 //prioridad del grupo en 150
D1(config-if)#standby 126 preempt // Habilite la preferencia
```

D1(config-if)#standby 126 track 4 decrement 60 //Rastree el objeto 4 ydecremeta 60
D1(config-if)#exit

Ilustración 14: show standby brief D1

The screenshot shows the GNS3 interface with a network diagram and a terminal window. The network diagram includes routers R1, R2, R3, and D1, along with PCs and VPCS. The terminal window displays the following configuration commands and output:

```

D1#conf ter
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 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#exit
D1#
Nov 26 05:16:28.020: %SYS-5-CONFIG_I: Configured from console by console
D1#show standby bri
D1#show standby brief
P indicates configured to preempt.

```

Interface	Grp	Pri	P State	Active	Standby	Virtual IP
Vl100	104	90	P Active	local	unknown	10.0.100.254
Vl100	106	90	P Active	local	unknown	FE80::5:73FF:FEA0:6
Vl101	114	40	P Init	unknown	unknown	10.0.101.254
Vl101	116	40	P Init	unknown	unknown	FE80::5:73FF:FEA0:7
Vl102	124	90	Init	unknown	unknown	10.0.102.254
Vl102	126	90	P Init	unknown	unknown	FE80::5:73FF:FEA0:7

Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

Tabla 5: Tabla tareas parte 5 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: admin • 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: \$trongPass
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 .

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

Se habilita en cada dispositivo la contraseña encriptada con el comando `enable algorithm-type scrypt secret cisco12345cisco`, ayuda a proteger un enrutador de ser comprometido por un ataque ya que si el atacante pasa la primera capa de defensa, la contraseña secreta de habilitación no le permite pasar.

```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

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

Se crea un usuario local como `sadmin` y se usa la contraseña del algoritmo de encriptación SCRYPT de ingreso con `cisco12345cisco`, con un nivel de privilegio de 15

```
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

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

Se habilita AAA mediante el comando `aaa new-model` en todos los dispositivos excepto R2

```
R1(config)#aaa new-model
R3(config)#aaa new-model
D1(config)#aaa new-model
D2(config)#aaa new-model
A1(config)#aaa new-model
```

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

Se configura en todos los dispositivos excepto en R2, el sistema de seguridad RADIUS que es un servidor o cliente distribuido para una red segura contra el acceso no autorizado según (ccna-learner.com, 2020), con la Dirección IP del servidor RADIUS es 10.0.100.6, Puertos UDP del servidor RADIUS son 1812 y 1813 y la contraseña: `$strongPass`

```
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 acct-port 1813
R1(config-radius-server)#key $strongPass
R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 acct-port 1813
R3(config-radius-server)#key $strongPass
D1(config)#radius server RADIUS
```

```

D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 acct-port 1813
D1(config-radius-server)#key $strongPass
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 acct-port 1813
D2(config-radius-server)#key $strongPass
A1(config)#radius server RADIUS
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 acct-port 1813
A1(config-radius-server)#key $strongPass

```

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

Se proporciona seguridad con AAA es un marco de trabajo estándar que se utiliza para controlar quién puede utilizar los recursos de la red (mediante autenticación), qué están autorizados a hacer (mediante autorización) y capturar las acciones realizadas mientras accede a la red (mediante contabilidad), AAA se implementó usando los servidores radius según (geeksforgeeks.org, s.f.)

```

R1(config)#aaa authentication login default group radius local
R3(config)#aaa authentication login default group radius local
D1(config)#aaa authentication login default group radius local
D2(config)#aaa authentication login default group radius local
A1(config)#aaa authentication login default group radius local

```

Tarea 5.6: Verifique el servicio AAA en todos los dispositivos (excepto R2).

Para verificar se cerraron e iniciaron todos los dispositivos excepto R2, ingresando con el usuario: raduser y la contraseña: upass123., por lo que se pudo ver que no es válido el usuario de ingreso, así como la contraseña.

Ilustración 15: Autenticación AAA R1 GNS3v

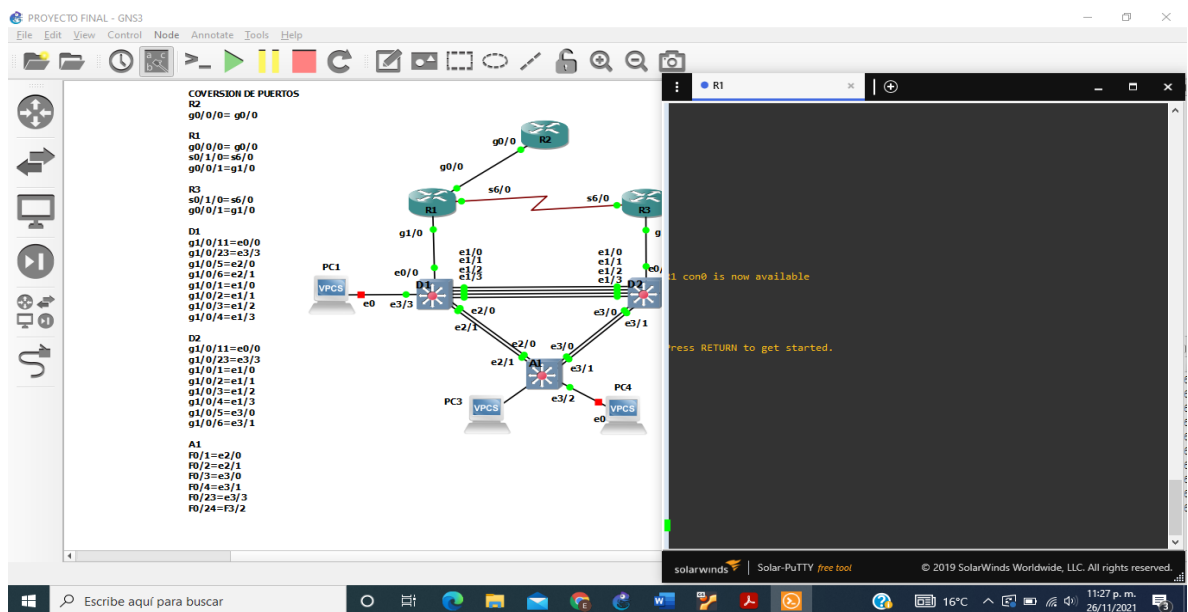


Ilustración 16: Autenticación AAA R3 GNS3

The screenshot shows the GNS3 interface with a network topology and a terminal window for router R3. The terminal output is as follows:

```

R3 con0 is now available.
Press RETURN to get started.

R3, ENCOR Skills Assessment, Scenario 1

User Access Verification
Username: raduser
Password:
% Authentication failed
Username:
    
```

The network topology includes routers R1, R2, R3, D1, D2, and A1, along with PCs and VPCS. The terminal window shows a successful connection to the console and a failed authentication attempt for user 'raduser'.

Ilustración 17: Autenticación AAA D1 GNS3

The screenshot shows the GNS3 interface with a network topology and a terminal window for device D1. The terminal output is as follows:

```

Press RETURN to get started.

*Nov 27 04:34:54.764: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R1 GigabitEthernet1/0 (full duplex).
*Nov 27 04:35:53.085: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R1 GigabitEthernet1/0 (full duplex). D1, ENCOR Skills Assessment, Scenario 1

User Access Verification
Username: raduser
Password:
% Authentication failed
Username:
*Nov 27 04:36:49.563: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R1 GigabitEthernet1/0 (full duplex).
Username:
    
```

The network topology is identical to the previous screenshot. The terminal window shows a successful connection to the console, followed by CDP error messages and a failed authentication attempt for user 'raduser'.

Ilustración 18: Autenticación AAA D2 GNS3

The screenshot displays the GNS3 interface with a network topology and a terminal window for router D2. The topology shows three routers (R1, R2, R3) and four PCs (PC1-PC4) connected via various interfaces. The terminal window shows the following output:

```

D2 con0 is now available
Press RETURN to get started.
*Nov 27 04:35:17.804: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet1/0 (full duplex).
*Nov 27 04:36:13.004: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet1/0 (full duplex).
*Nov 27 04:37:12.888: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet0/0 (not full duplex), with R3 GigabitEthernet1/0 (full duplex). D2, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username:
Password:
% Authentication failed
Username:
    
```

The interface also shows a configuration table for port conversion:

Router	Local Interface	Remote Interface
R2	g0/0/0	g0/0
R1	g0/0/0	g0/0
R1	e0/1/0	s6/0
R1	g0/0/1	g1/0
R3	s0/1/0	s6/0
R3	g0/0/1	g1/0
D1	g1/0/11	e0/0
D1	g1/0/23	e3/3
D1	g1/0/5	e2/0
D1	g1/0/6	e2/1
D1	g1/0/1	e1/0
D1	g1/0/2	e1/1
D1	g1/0/3	e1/2
D1	g1/0/4	e1/3
D2	g1/0/11	e0/0
D2	g1/0/23	e3/3
D2	g1/0/1	e1/0
D2	g1/0/2	e1/1
D2	g1/0/3	e1/2
D2	g1/0/4	e1/3
D2	g1/0/5	e3/0
D2	g1/0/6	e3/1
A1	f0/1	e2/0
A1	f0/2	e2/1
A1	f0/3	e3/0
A1	f0/4	e3/1
A1	f0/23	e3/3
A1	f0/24	f3/2

Ilustración 19: Autenticación AAA A1 GNS3

The screenshot displays the GNS3 interface with a network topology and a terminal window for router A1. The topology is identical to the previous image. The terminal window shows the following output:

```

A1 con0 is now available
Press RETURN to get started.
A1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: raduser
Password:
% Authentication failed
Username:
    
```

The interface also shows the same configuration table for port conversion as in the previous image.

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: Tareas parte 6 Configure las funciones de Administración de 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	Especificaciones de SNMPv2: <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>traps config</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> .

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

Se configura el reloj local a la hora UTC actual de cada dispositivo

```
R1#clock set 09:35:00 nov 28 2021
R2#clock set 09:37:00 nov 28 2021
R3#clock set 09:39:00 nov 28 2021
D1#clock set 09:40:00 nov 28 2021
```

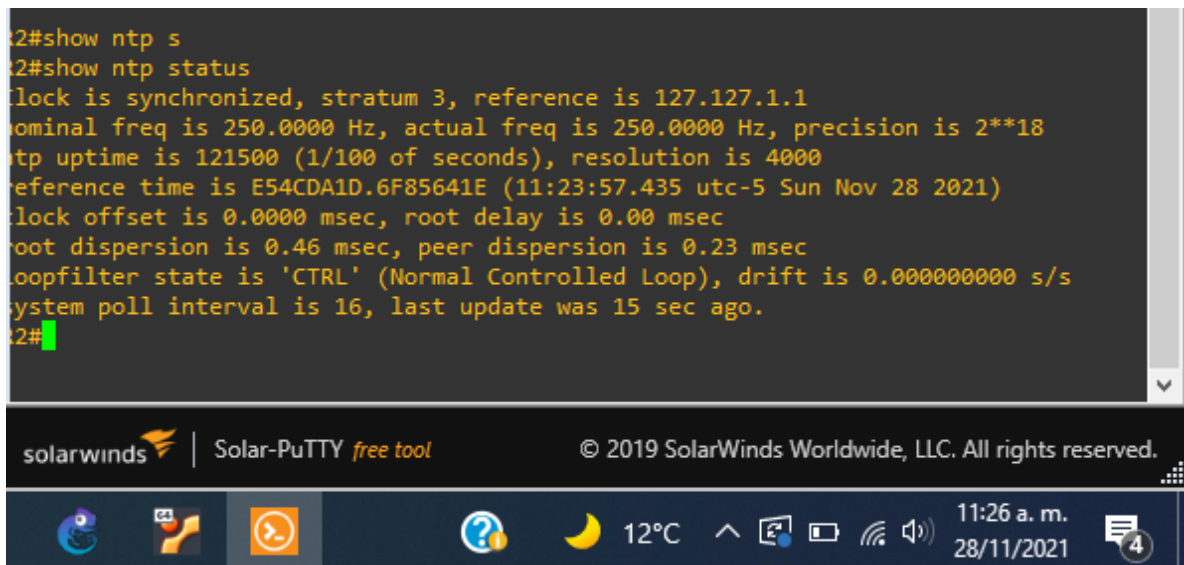
```
D2#clock set 09:40:00 nov 28 2021
A1#clock set 09:41:00 nov 28 2021
```

Tarea 6.2: Configure R2 como un NTPmaestro.

Se configura el router 2 con NTP maestro en nivel de estrato 3 con el siguiente comando

```
R2(config)#ntp master 3
R2(config)#exit
```

Ilustración 20: show NTP status R2



```
R2#show ntp s
R2#show ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.1
Nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
ntp uptime is 121500 (1/100 of seconds), resolution is 4000
reference time is E54CDA1D.6F85641E (11:23:57.435 utc-5 Sun Nov 28 2021)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.46 msec, peer dispersion is 0.23 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 15 sec ago.
R2#
```

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

Se configura NTP según la guía con R1 sincronizado con R2, los dispositivos R3, D1 y A1 se sincronizo la hora con R1, y el switch D2 se sincronizara la hora con R3.

```
R1(config)#ntp server 2.2.2.2
R3(config)#ntp server 10.0.10.1
D1(config)#ntp server 10.0.10.1
A1(config)#ntp server 10.0.10.1
D2(config)#ntp server 10.0.11.1
```

Ilustración 21: show NTP associations R1

```
R1#show ntp a
R1#show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
*~2.2.2.2      127.127.1.1    3   29    64    1  9.225  -0.191 189.61
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

11:28 a. m. 28/11/2021

Ilustración 22: show NTP associations R3

```
R3#show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.10.1     .INIT.         16  -     512   0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R3#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

11:30 a. m. 28/11/2021

Ilustración 23: show NTP associations D1

```
D1#show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
*~10.0.10.1    2.2.2.2        4   15    64    1  9.240  -684558 3938.5
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
D1#
Nov 28 11:31:38.355: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Etherne
t0/0 (not full duplex), with R1 GigabitEthernet1/0 (full duplex).
D1#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

11:31 a. m. 28/11/2021

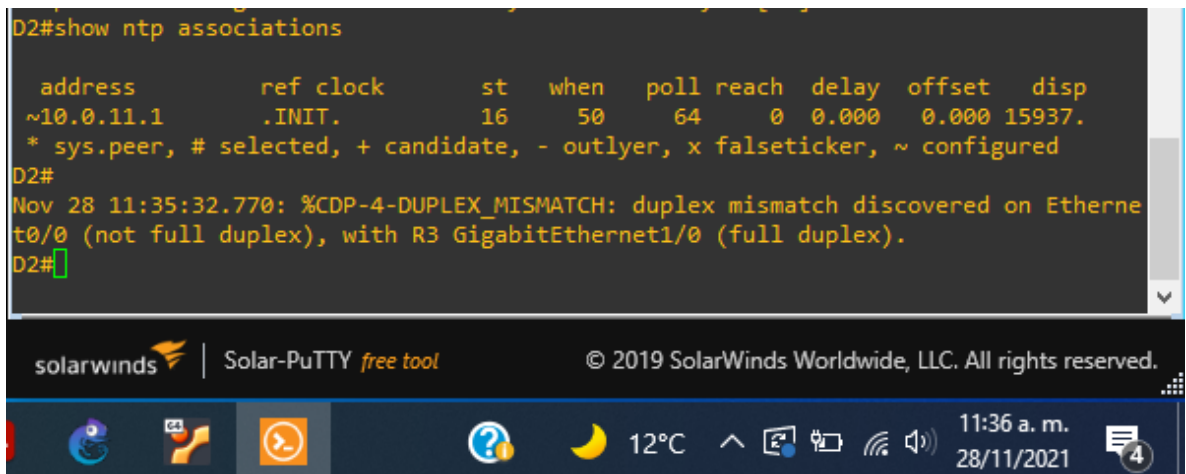
Ilustración 24: show NTP associations A1



```
A1#
Nov 27 16:33:17.596: %SYS-5-CONFIG_I: Configured from console by sadmin on console
A1#show ntp as
A1#show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.10.1     .INIT.         16   -     512    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
A1#
```

Ilustración 25: show NTP associations D2



```
D2#show ntp associations

  address      ref clock      st  when  poll reach  delay  offset  disp
~10.0.11.1     .INIT.         16   50   64    0  0.000  0.000 15937.
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
D2#
Nov 28 11:35:32.770: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Etherne
t0/0 (not full duplex), with R3 GigabitEthernet1/0 (full duplex).
D2#
```

Tarea 6.4: Configure Syslog en todos los dispositivos excepto R2

Se configura Syslogs en todos los dispositivos excepto en R2 los cuales deben enviar a la PC1 en 10.0.100.5 en el nivel WARNING.

```
R1(config)#logging trap warning
R1(config)#logging host 10.0.100.5
R1(config)#logging on
```

```
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5
R3(config)# logging on
```

```
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5
```

```
D1(config)#logging on
```

```
D2(config)#logging trap warning  
D2(config)#logging host 10.0.100.5  
D2(config)#logging on
```

```
A1(config)#logging trap warning  
A1(config)#logging host 10.0.100.5  
A1(config)#logging on
```

Tarea 6.5: Configure SNMPv2c en todos los dispositivos excepto R2

Se configura SNMPv2 en todos los dispositivos excepto en R2, usándolo de solo lectura, se limitó el acceso SNMP a la dirección 10.0.100.5 del PC1, se configuro el valor de contacto de SNMP con urieltibocha, se establece community string en ENCORSA, también en R3, D1 y D2 se habilito él envió de traps config y ospf, en R1 el envío de traps bgp, config y ospf y en A1 traps config.

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

```
R3  
R3(config)# logging on  
R3(config)#ip access-list standard SNMP-NMS  
R3(config-std-nacl)#permit host 10.0.100.5  
R3(config-std-nacl)# exit  
R3(config)#snmp-server contact Cisco urieltibocha  
R3(config)#snmp-server community ENCORSA ro SNMP-NMS  
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA  
R3(config)#snmp-server enable traps ospf  
R3(config)#snmp-server enable traps config  
R3(config)#end
```

```
D1  
D1(config)#ip access-list standard SNMP-NMS  
D1(config-std-nacl)#permit host 10.0.100.5  
D1(config-std-nacl)#exit  
D1(config)#snmp-server contact Cisco urieltibocha
```

```

D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps ospf
D1(config)#snmp-server enable traps config //swicht no permite Habilita traps
config

D1(config)#end

D2
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#exit
D2(config)#snmp-server contact Cisco urieltibocha
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server ifindex persist
D2(config)#snmp-server enable traps ospf
D2(config)#snmp-server enable traps config //swicht no permite habilitar traps
config

D2(config)#end

A1
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco urieltibocha
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server ifindex persist
A1(config)#snmp-server enable traps config //swicht no permite habilitar traps
config

A1(config)#end

```

CONCLUSIONES

Se logra concluir con el desarrollo de esta práctica como escenario de configuración de una topología de red, que se debe determinar e identificar que dispositivos son los necesarios con las especificaciones que se proyectan para que soporte cada comando de aplicación para los diferentes protocolos que se desean implementar.

Se logra concluir que para habilitar OSPFv3 en los dispositivos activos de red se debe configurar primeramente una ip para cada interfaz que se desea aplicar este protocolo, así mismo quedara habilitado para ser interconectado mediante este protocolo con otros dispositivos

Con la simulación de GNS3 se logra evidenciar que los equipos de computo a utilizar por este simulador deben tener una capacidad mínima de 8G de RAM, con el fin de que no se bloquee y pueda realizar la configuración sin tener percances de velocidad y bloqueo del equipo.

Con la configuración de OSPFv2 y OSPFv3 se logra determinar que cada protocolo hace referencia ya sea IPV4 con su respectivo direccionamiento, e IPV6 según sea el caso con su respectivo enrutamiento, por lo cual los dispositivos se deben identificar y seleccionar con el fin de que soporten estos protocolos.

BIBLIOGRAFÍA

ccna-learner.com. (27 de 12 de 2020). *ccna-learner.com*. Recuperado el 26 de 11 de 2021, de <https://www.ccna-learner.com/2020/12/27/radius-configuration-on-cisco-router-lab-radius-configure-and-improve-your-ski/>

computerweekly.com. (s.f.). *computerweekly.com*. Recuperado el 27 de 11 de 2021, de <https://www.computerweekly.com/es/consejo/Networking-redes-cableado-Similitudes-y-diferencias>

ecured.com. (s.f.). *ecured.com*. Recuperado el 27 de 11 de 2021, de [https://www.ecured.cu/Conmutaci%C3%B3n_\(Redes_de_comunicaci%C3%B3n\)](https://www.ecured.cu/Conmutaci%C3%B3n_(Redes_de_comunicaci%C3%B3n))

geeksforgeeks.org. (s.f.). *www.geeksforgeeks.org*. Recuperado el 26 de 11 de 2021, de <https://www.geeksforgeeks.org/aaa-authentication-authorization-and-accounting-configuration-locally/>

tecnoseguro.com. (s.f.). *tecnoseguro.com*. Recuperado el 27 de 11 de 2021, de <https://www.tecnoseguro.com/tutoriales/fundamentos-enrutamiento-draytek>

universidad complutense. (s.f.). *universidad complutense*. Recuperado el 27 de 11 de 2021, de <https://www.ucm.es/pimcd2014-free-software/gns3>