DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GERMAN ARTURO VILLARREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERA ELECTRÓNICA
SINCELEJO - SUCRE
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GERMAN ARTURO VILLARREAL

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR POR EL TÍTULO DE INGENIERO ELECTRÓNICO

DIRECTOR:

MSC. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERA ELECTRÓNICA

SINCELEJO - SUCRE

2021

Nota de Aceptación

Firma presidente del Jurado

Firma del jurado

Firma del Jurado

Bogotá (10, diciembre, 2021)

AGRADECIMIENTOS

En primer lugar quiero dar gracias a Dios por ser guía y apoyo en cada instante de mi vida, gracias a él por la oportunidad de aprender a ser cada día una mejor persona, gracias a la vida que a diario me demuestra lo maravillosa que puede ser, gracias a los docentes porque con su conocimiento y apoyo enriquecieron a diario mi conocimiento y formación profesional, gracias a mis padres y familiares por ser pilar de mi crecimiento y estar conmigo de manera continua , finalmente quiero agradecer a la Universidad nacional abierta y a distancia por ser una oportunidad de enseñanza para las personas trabajadoras y emprendedoras del país.

TABLA DE CONTENIDO

Lista de tablas

Lista de Figuras

GLOSARIO

CISCO: Es una empresa global que centra su funcionamiento en la fabricación de dispositivos para redes de comunicación, soluciones a las problemáticas que se puede presentar en el servicio de configuración de redes.

PACKET TRACER: Programa de simulación de topologías de red, que permite verificar el funcionamiento y conectividad en la tipología de una red.

CCNP: Se denomina así a la certificación de manejo infraestructura de red e internet emitida por CISCO.

EIGRP: Protocolo de enrutamiento de prueba que utiliza un vector distancia en una configuración de red con el fin de encontrar la ruta más próxima.

ETHERCHANNEL: Es una tecnología, que permite interconectar, switches, routers, servidores, etc.

LACP: Protocolo utilizado con el fin de regular los enlaces e incrementar el ancho de banda entre los dispositivos involucrados

OSPF: Protocolo de direccionamiento para redes IP, el cual tiene como propósito, encontrar la ruta más rápida entre dos nodos de una red.

VLAN: (Red de Área Local Virtual). Tecnología de red que permite la creación de redes lógicas independientes en una misma red.

ENRUTAMIENTO: Función que desempeña el Router con el fin de descubrir el camino más viable para enviar una red de paquetes.

CONMUTACIÓN: Se considera así a el establecimiento de una vía de dos puntos uno denominado emisor y el otro receptor con el fin de enviar datos de un punto a otro de manera directa.

RESUMEN

Con el fin de obtener el título de ingeniero electrónico de la Universidad Nacional abierta y a distancia (UNAD) el presente escrito pretende desarrollar de manera adecuada las habilidades teóricas y prácticas, necesarias para desarrollar el diplomado CCNP Cisco y cumplir a cabalidad con el desarrollo de cada uno de los escenarios propuestos por la dirección del diplomado para lograr adecuadamente el desarrollo de una topología de redes.

En esta oportunidad el desarrollo del proyecto se centró en la realización de una topología de red basada en tres Router, que demandaron el uso de dos switches capa 3 modelo 3650, uno modelo 2960 y cuatro ordenadores finales para poder cumplir a cabalidad con el desenvolvimiento de esta red. Asimismo, fue necesario enfatizar en las temáticas de direccionamiento IPV 4 e IPV 6, hacer uso de protocolos de enrutamiento como el OSPF y el BGP configurados entre distintos routers y switch de modelo 3 junto a unas VLANs, canales de tensiones y distintos protocolos de spanning tree de la capa 2 del modelo OSI configurados en distintos switch de la capa 3 para poder realizar de manera adecuada el funcionamiento de estas redes quienes se activan o desactivan automáticamente los enlaces de comunicación.

Con base en lo anterior, el documento presente tiene la función de describir paso a paso el procedimiento necesario para poder configurar mediante distintas clases de código los puntos necesarios para el envío y recepción de datos por medio de una topología de red programada en Packet Tracer que hace uso de distintos comandos con el fin de verificar las conexiones y la conmutación entre las topologías de redes que permiten validar el estado en el que el cual se encuentra la red.

Palabras clave: Cicso,Packet Tracer,Ccnp,Eigrp,Eterchannel,Lacp,Ospf,Vlan,Router,Switch.

ABSTRACT

In order to obtain the title of electronic engineer from the Open and Distance National University (UNAD), this document aims to adequately develop the theoretical and practical skills necessary to develop the Cisco CCNP diploma and fully comply with the development of each one of the scenarios proposed by the management of the diploma to adequately achieve the development of a network topology.

On this occasion, the development of the project focused on the realization of a network topology based on three routers, which required the use of two layer 3 switches model 3650, one model 2960 and four final computers to be able to fully comply with the development of It's red. Likewise, it was necessary to emphasize the IPV 4 and IPV 6 addressing issues, make use of routing protocols such as OSPF and BGP configured between different routers and model 3 switches together with VLANs, voltage channels and different spanning protocols. tree of layer 2 of the OSI model configured in different switches of layer 3 to be able to carry out the proper operation of these networks, which automatically activate or deactivate the communication links.

Based on the above, the present document has the function of describing step by step the necessary procedure to be able to configure, through different types of code, the points necessary for sending and receiving data through a network topology programmed in Packet Tracer that makes use of different commands in order to verify the connections and the switching between the network topologies that allow to validate the state in which the network is located.

Keywords:Cicso,Packet Tracer,Ccnp,Eigrp,Eterchannel,Lacp,Ospf,Vlan,Router,Switch.

INTRODUCCIÓN

Con el fin de dar a conocer los aprendizajes teóricos y prácticos obtenidos a lo largo del diplomado en profundización de CCNP CISCO, de ingeniería en electrónica el presente trabajo evidencia el desarrollo de una red privada por medio de cada uno de los conocimientos obtenidos a lo largo del diplomado que permiten optar al título de ingeniero electrónico. El desarrollo de esta red privada tiene como fin implementar una topología de Router y switch que demanda la configuración de canales de VLANS, protocolos OSPF, comunicación dirigida, el uso troncal por medio de saltos y el establecimiento de canales EtherChannel, esto se logra, mediante la configuración de enrutamiento de IP V 4 e IPV 6 y el uso de un protocolo spanning Tree.

Con base en todo lo anterior y teniendo en cuenta que ya se han utilizado los protocolos anteriormente mencionados , que éstos permiten y promueven las actividades de enrutamiento de formas óptimas para el uso de las redes y la comunicación entre distintos routers se ha realizado una topología más amplia que permita configurar cada uno de estos dispositivos como routers switches en la capa 3 teniendo y los direccionamientos mencionados de manera autónoma en el cual se puede condensar el desarrollo óptimo de la red teniendo en cuenta los aprendizajes obtenidos en este diplomado .

Escenario Propuesto

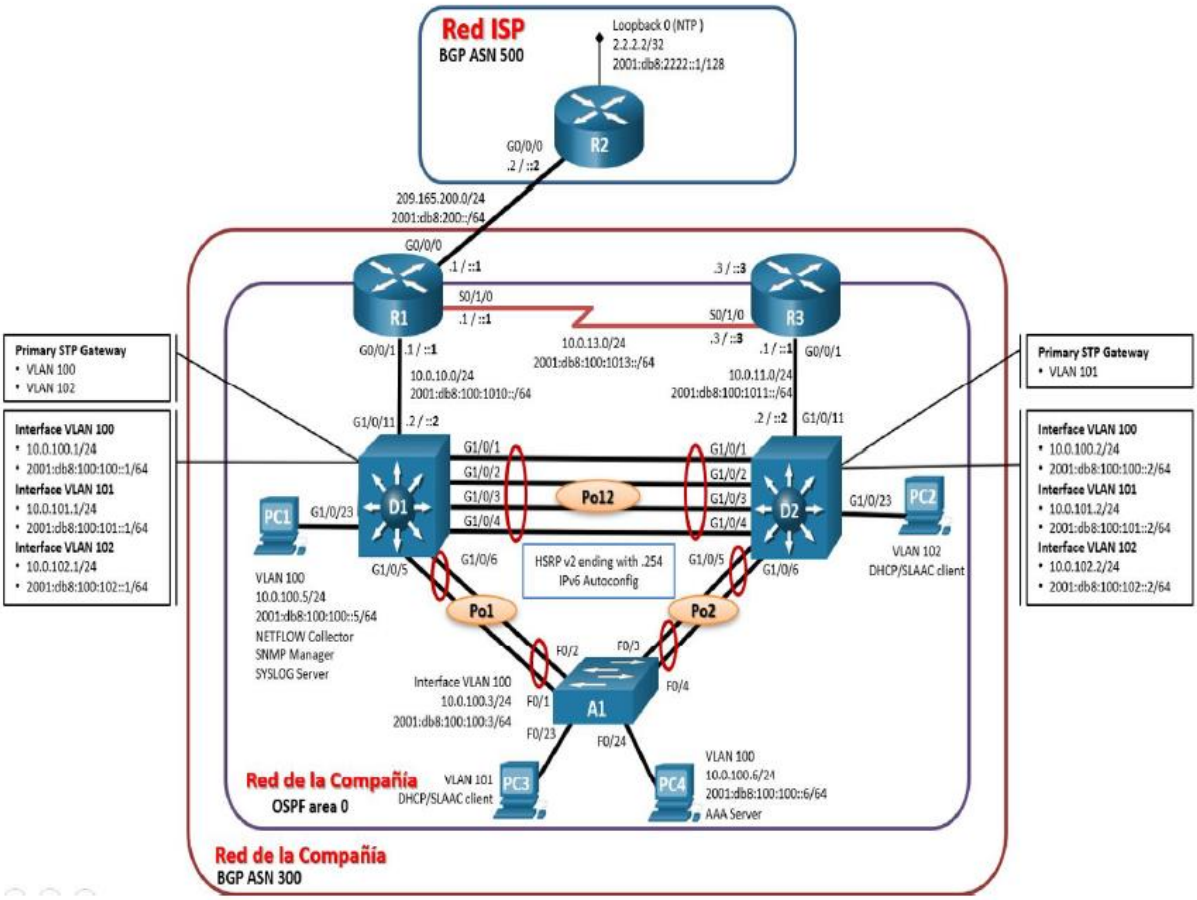


Figura 1 Topología modelo para la implementación.

Tabla de enrutamiento.

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
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

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

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

Para el montaje de la topología se utilizó las imágenes para los equipos Cisco L2 yL3 para el aplicativo Packet Tracert. Se realiza la conexión de puertos conforme a la topología indicada.

Montaje de la Topología propuesta mediante el aplicativo Packet Tracert y soporte de imágenes IOS de los dispositivos con VMWARE Workstation.

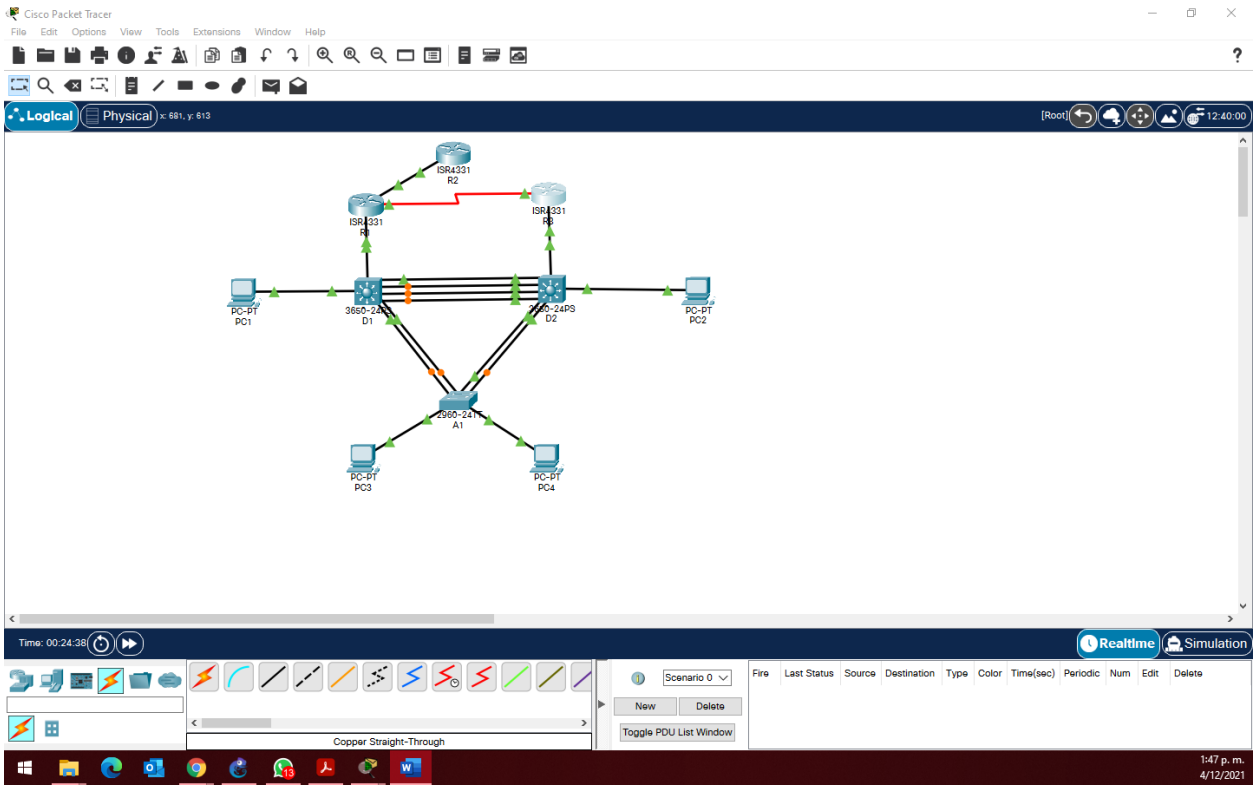


Figura 2 Paso 1 Montaje topología en aplicativo Packet Tracert

Paso 2 Configurar los parámetros básicos para cada dispositivo.

Configuraciones básicas en los Router.

En los routers (R1, R2, R3) Se realizará la configuración de única difusión por medio de protocolo ipv6, desactivación de la traducción de nombres del dispositivo lo cual evita problemas y traumatismos en los tiempos de configuración al momento de ingresar por error líneas de comando incorrectas, parametrización de direccionamiento en las interfaces de tal forma que se configure IPv4, IPv6 y la dirección IPv6 Link local para cada interfaz.

Comandos utilizados en R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.225 255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown

exit interface g0/0/1
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
```

Validación configuración ingresada R1

Comando utilizado: # Show ip interface brief

Este comando nos permite obtener un resumen de las interfaces del Router, detallando información parametrizada como direccionamiento ip en cada interfaz y el estado de estas.

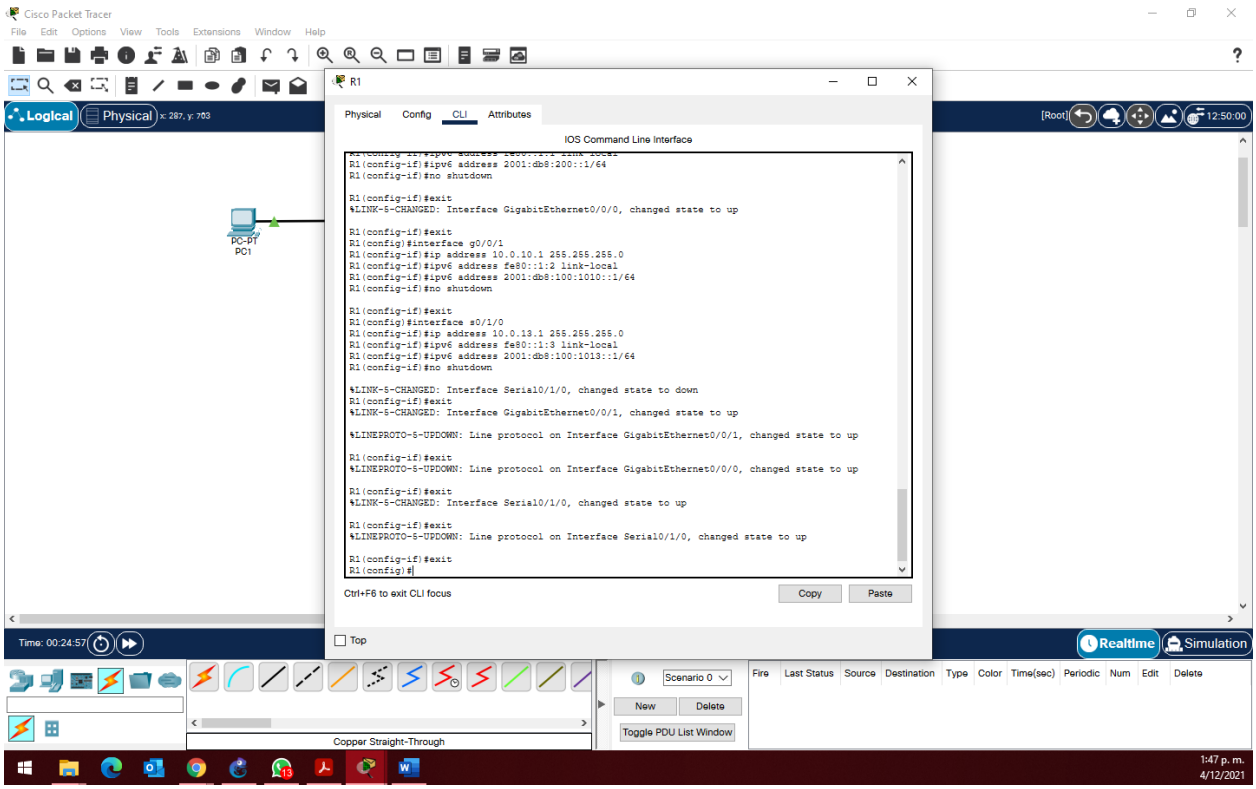


Figura 3 Paso 2 validación configuración R1

Comandos utilizados en R2

hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local

ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit

Validación configuración ingresada R2

Comando: # Show ip interface brief

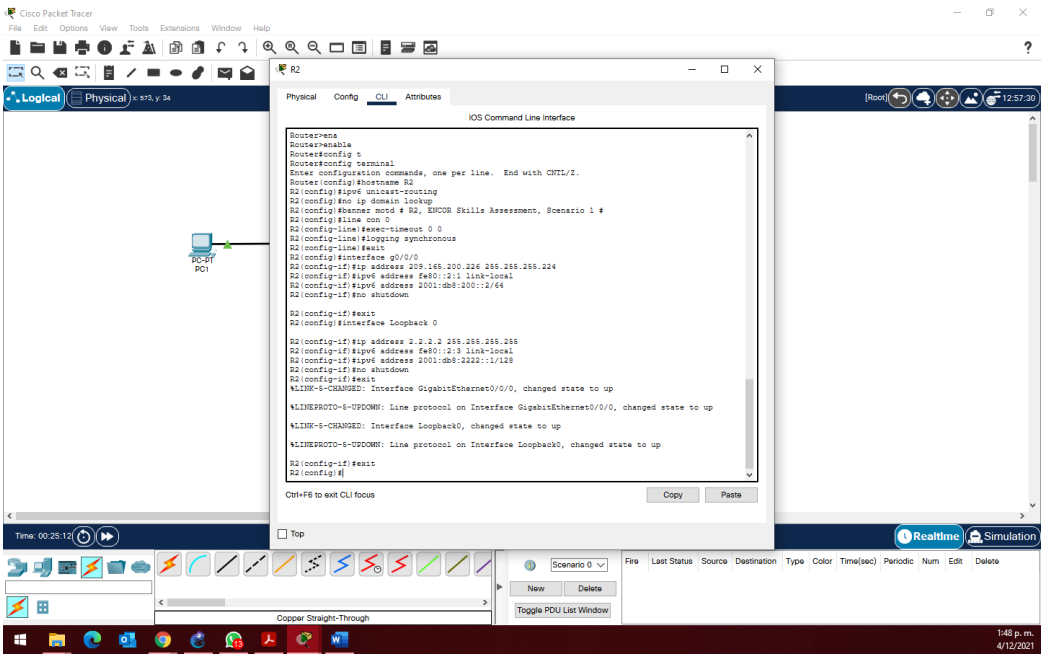


Figura 4 Paso 2 validación configuración R2

Comandos utilizados en R3

hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local

ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

Validación configuración ingresada R3

Comando: # Show ip interface brief

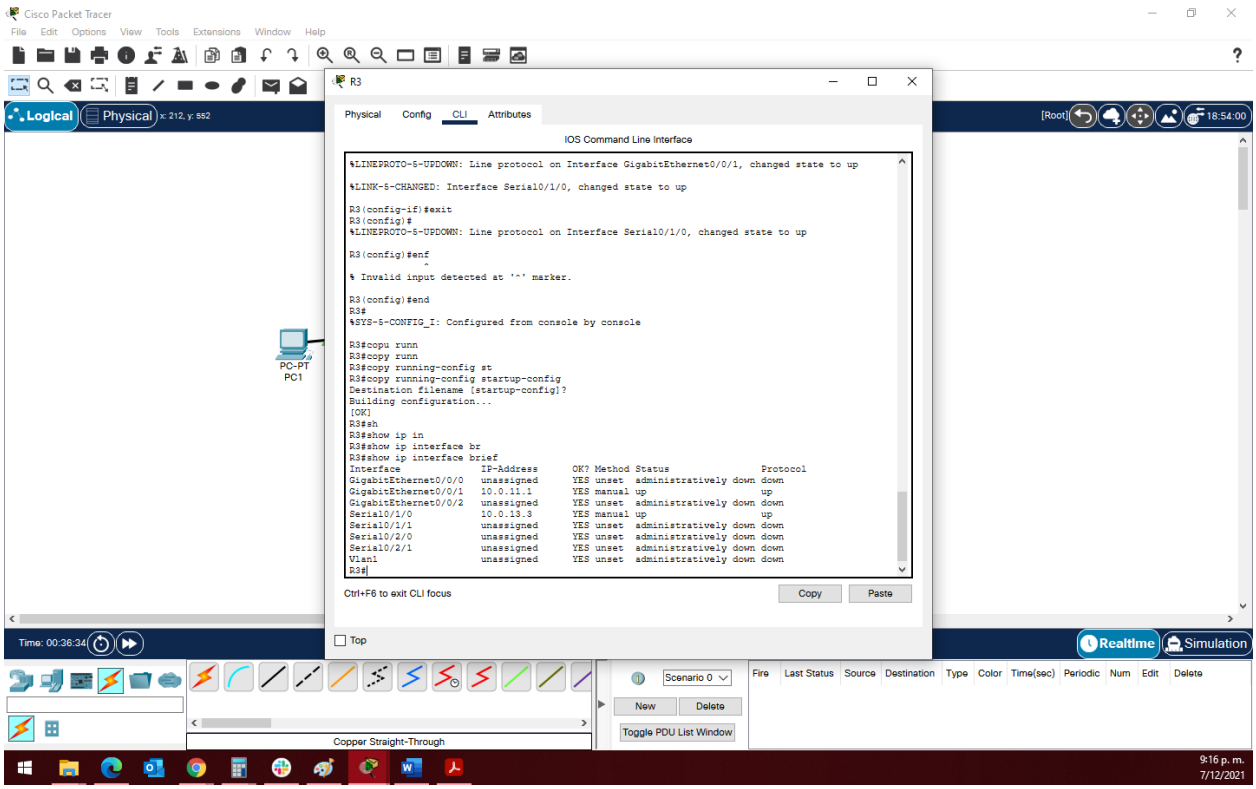


Figura 5 Paso 2 validación configuración R3

Configuraciones básicas para los Switch

Se realiza configuración de única difusión por medio de protocolo ipv6, desactivación de la traducción de nombres del dispositivo, creación de VLANs conforme a lo establecido en los

lineamientos del escenario (vlan 100, vlan 101, vlan 102) y su respectiva configuración de interfaces con parametrización IPv4, IPv6y exclusión de direcciones ip.

Comandos utilizados en D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
```

```
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Validaciones en D1

Comando**:** #Show running-config

Este comando permite visualizar información general completa de la terminal comoversiones, parámetros de configuración y direccionamiento de interfaces.

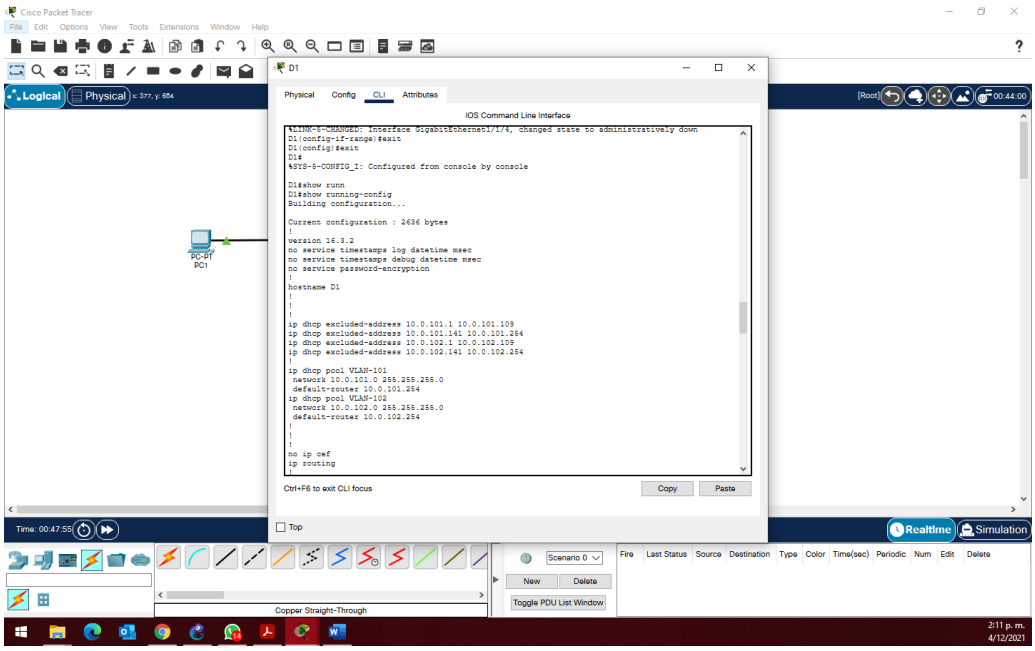


Figura 6 Paso 2 validación configuración D1

Comando: #show vlan brief

Este comando visualiza la asignación de puertos conforme a las v LAN creadas y alconjunto de subredes IP configuradas.

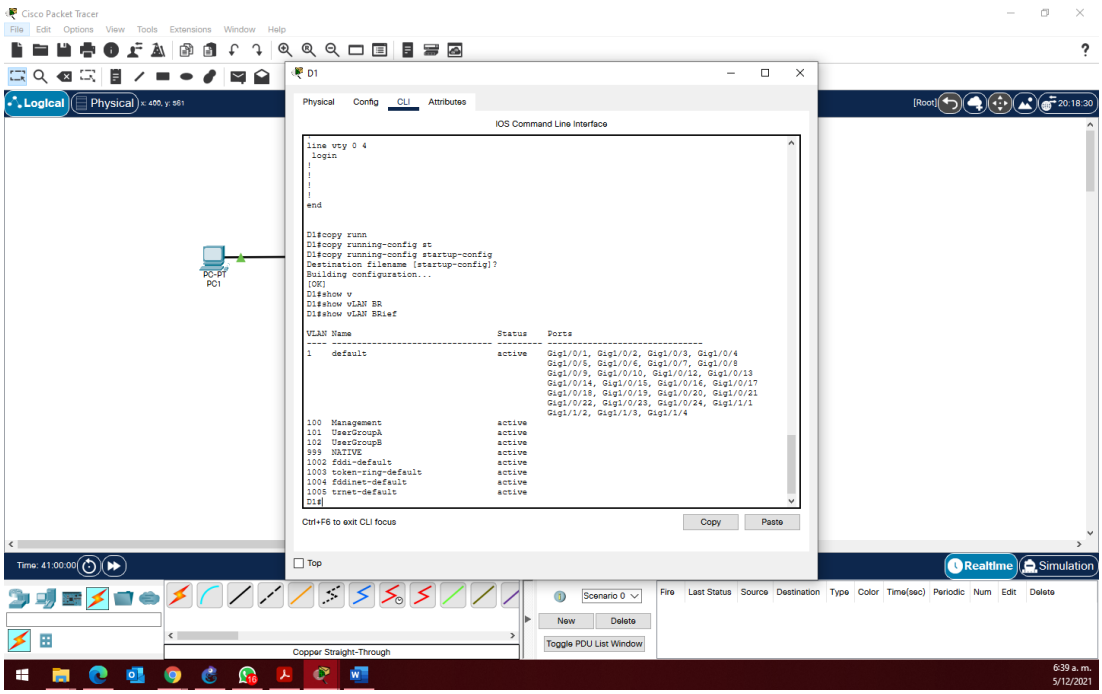


Figura 7 Paso 2 validación configuración D1

Comandos utilizados en D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
```

```
interface g1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Validaciones en D2

Comando: #Show running-config

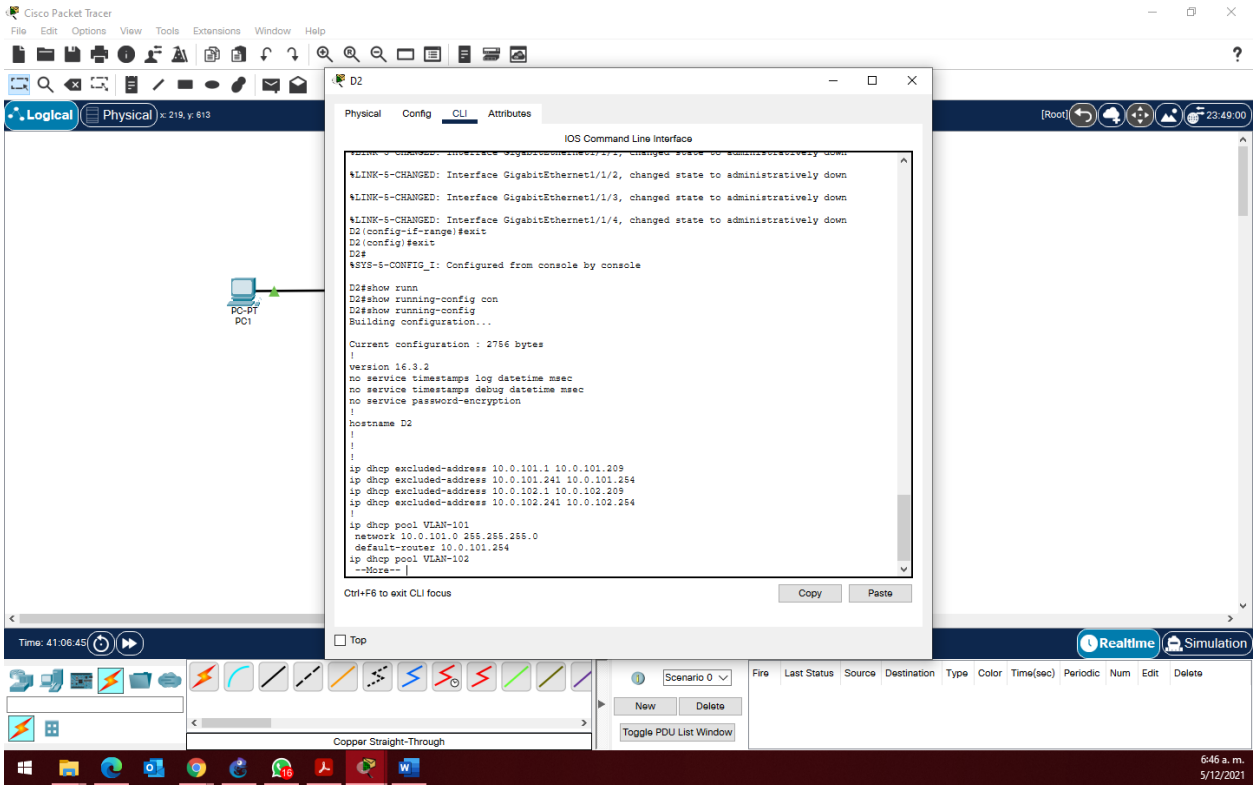


Figura 8 Parte1-Paso 2 validación configuración D2

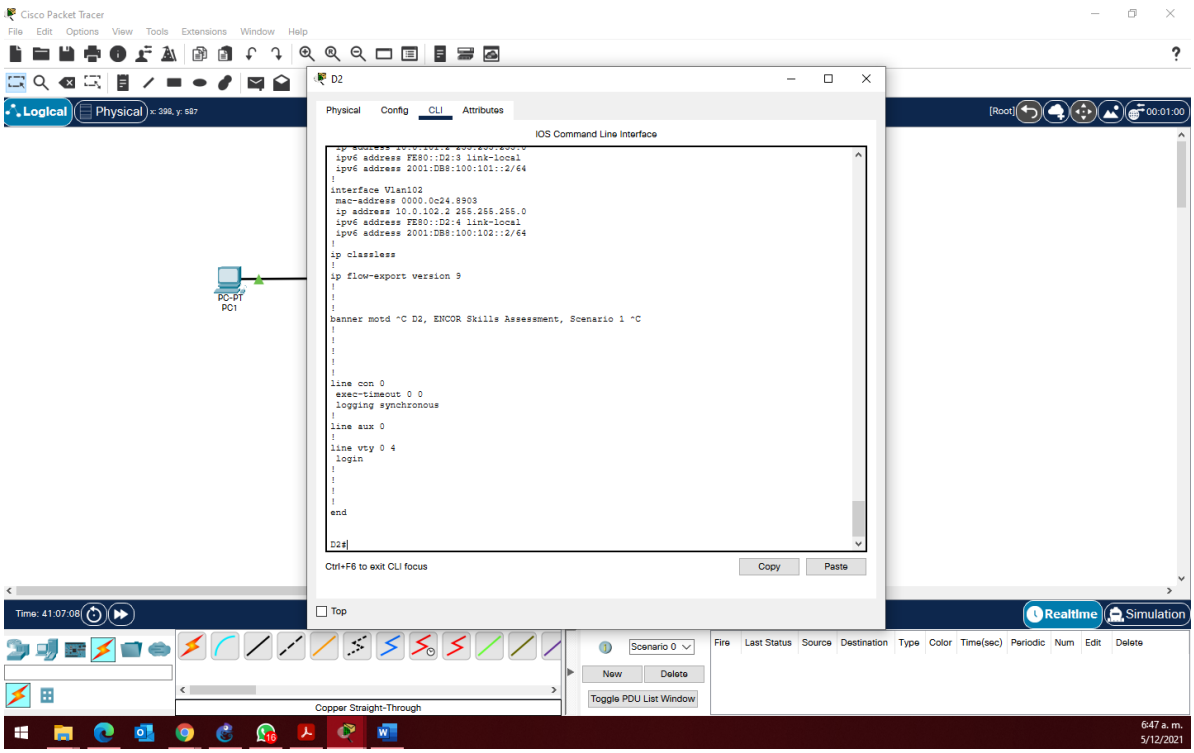


Figura 9 Parte 1-Paso 2 validación configuración D2

Comandos utilizados en Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
```

ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
exit

Validaciones en A1

#show running-config

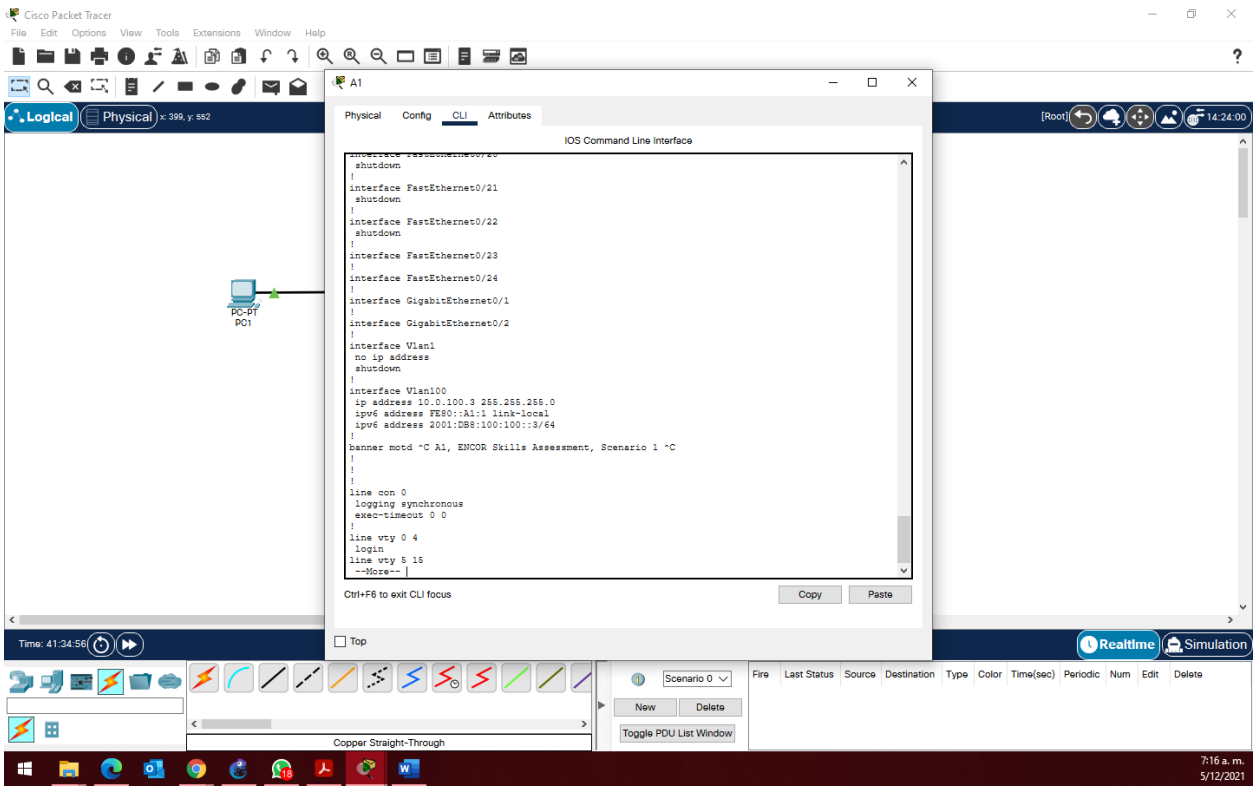


Figura 10 Parte 1-Paso 2 validación configuración A1

Configuración equipos PC1

Se realiza la configuración estática de direcciones según la tabla de direccionamiento tanto en IPV4 como en IPV6 en los terminales PC1 Y PC4

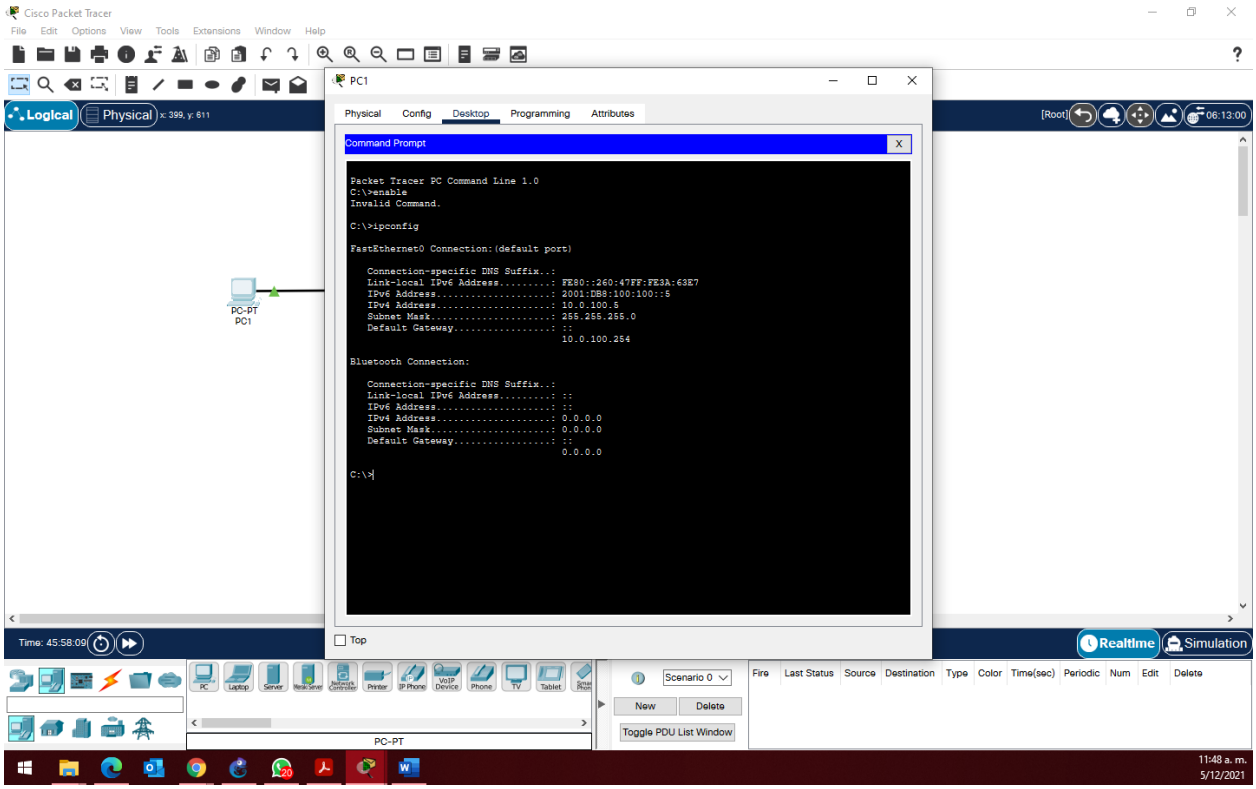


Figura 11 Parte 1-Paso 2 configuración IP PC1

Configuración equipos PC4

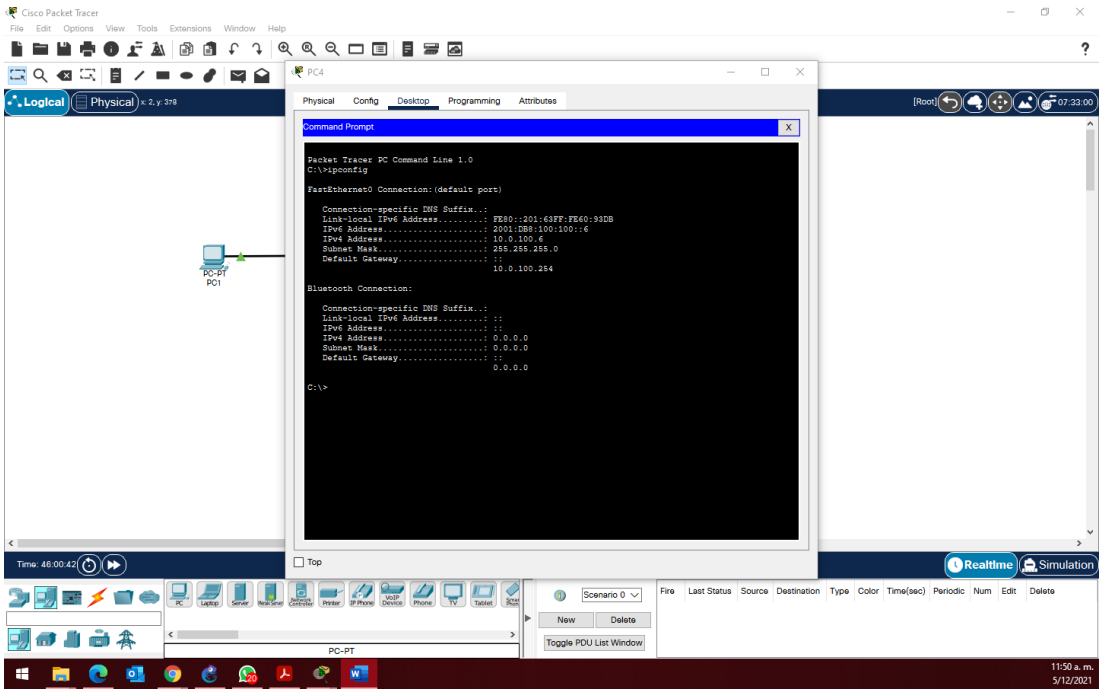


Figura 12 Parte 1-Paso 2 configuración IP PC4

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

En esta parte se realizará los siguientes puntos:

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

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

2.3 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.

2.4 D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

Se procede a parametrizar el protocolo de encapsulamiento **IEEE 802.1q** el cual permite la interacción de diversas redes por un mismo medio físico, de igual manerase realiza la configuración del protocolo **RSTP** en busca de obtener un mejor tiempode respuesta para enlace de convergencia de la Topología de red.

Configuración en D1

Comandos utilizados en D1:

Enable

Config t

spanning-tree mode rapid-pvst spanning-tree vlan 100 root primary spanning-tree vlan 102 root primary spanning-tree vlan 101 root secondaryexit

interface range G1/0/1-6

switchport trunk encapsulation dot1q
switchport mode trunk

switchport trunk native vlan 999

Validaciones en D1

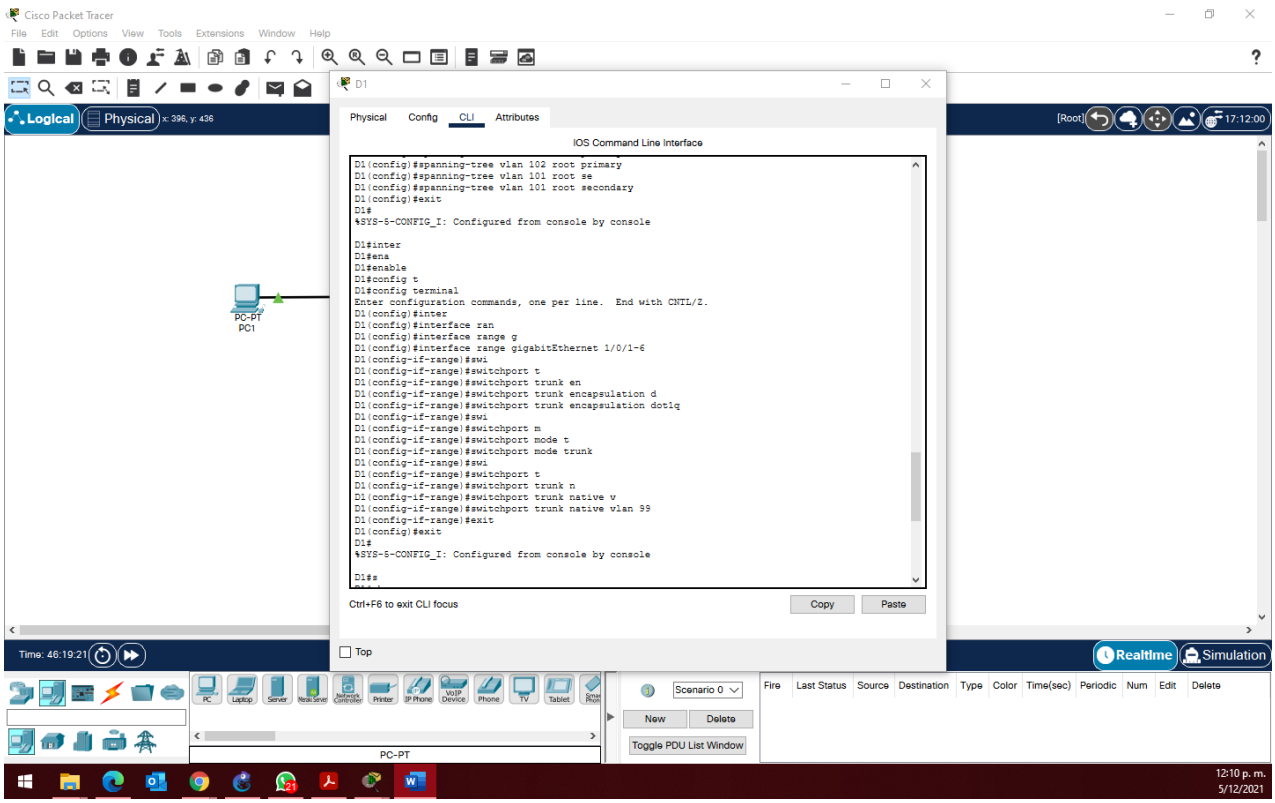


Figura 13 Parte 2-Paso 2 configuración D1 IEEE802.1q

Validación protocolo rapid spanning tree en D1

Comando: show spanning-tree:

Validación de enlaces de conexión

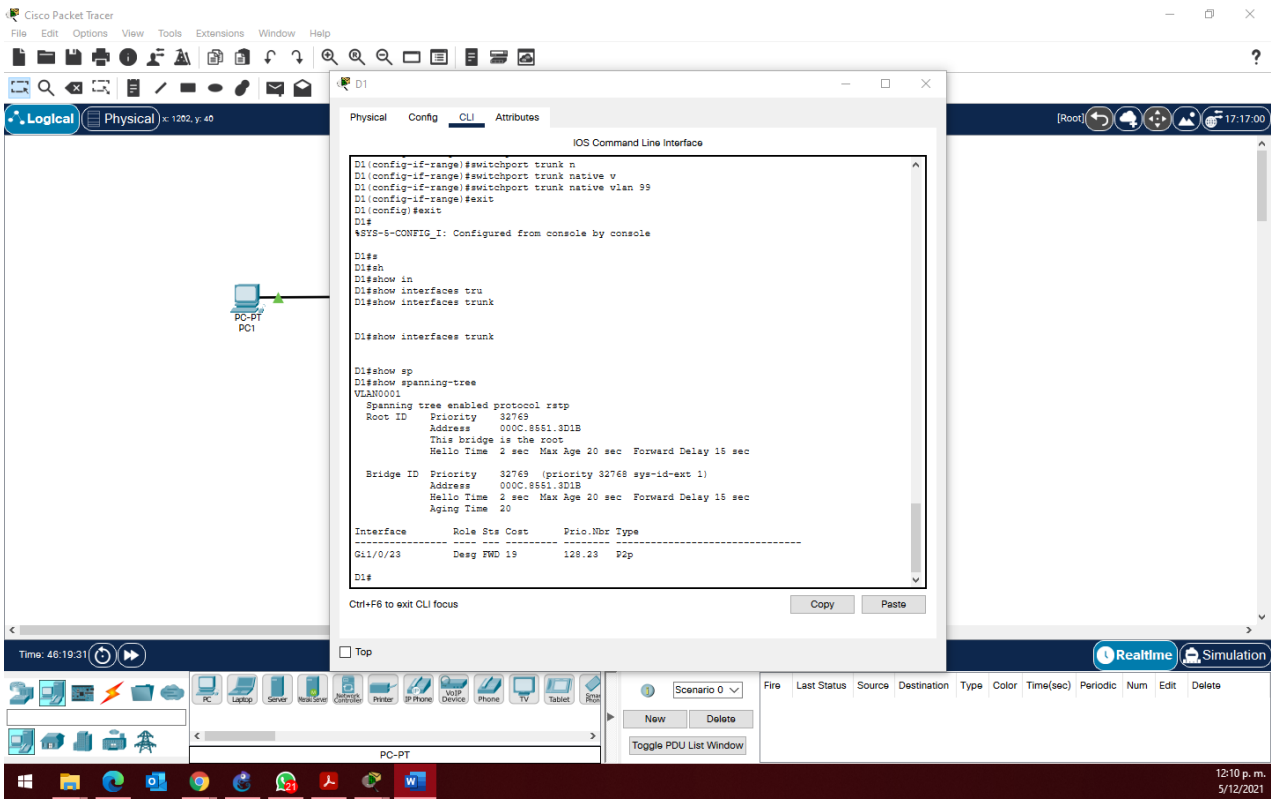


Figura 14 Parte2 validación RSTP en D1

Configuración en D2

Comandos utilizados:

Enable
Config t

spanning-tree mode rapid-pvst

spanning-tree vlan 101 root primary

spanning-tree vlan 100,102 root secondary

interface range G1/0/1-6

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 999

Validación de configuración en D2

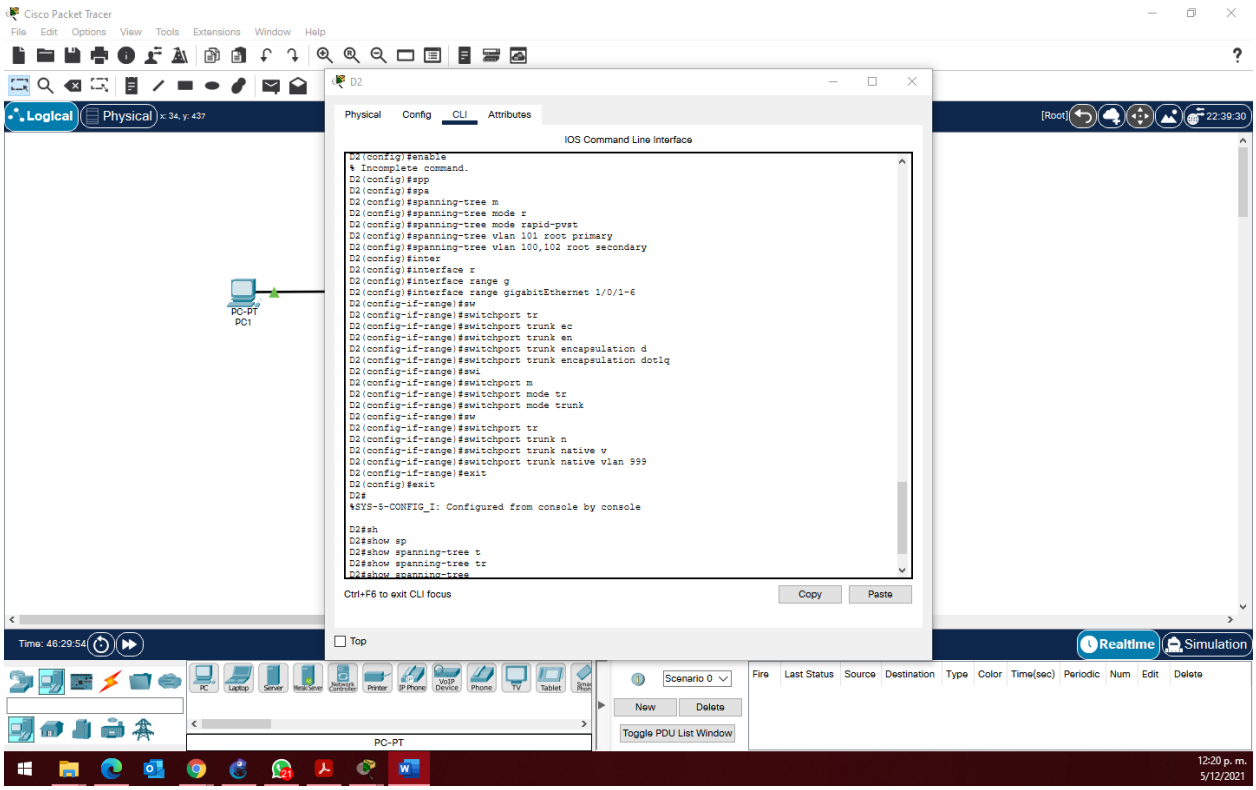


Figura 15 Parte2 validación RSTP en D2

Configuración en A1

Comandos utilizados:

Enable

Config t

spanning-tree mode rapid-pvst

interface range F 0/1-4

switchport mode trunk switchport trunk

native vlan 999

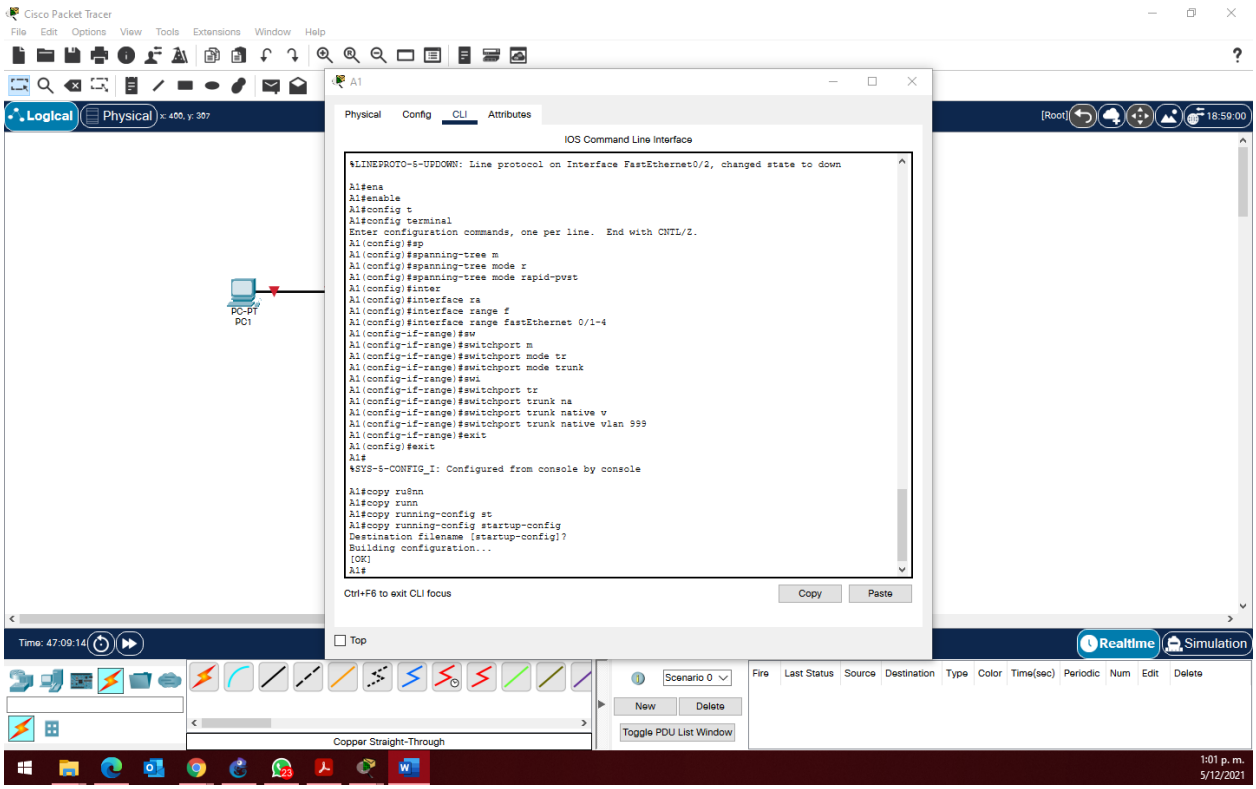


Figura 16 Parte2 configuración spanning- tree A1

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

La creación de EtherChannel en nuestra Topología nos permite agrupar una serie de enlaces físicos entre los Switch en un solo enlace lógico con el fin de permitir una velocidad de transmisión mayor, para este caso se utiliza el protocolo de negociación LACP (Link aggregation control protocol) el cual es de uso libre y registrado bajo la IEEE.

Creacion PortChannel #12 y #1 en switch D1

Configuración portchannel 12 D1

Enable

Config t

Interface range G1/0/1-4

Switchport mode trunk channel-
protocol LACP channel-group 12
mode active no shutdown

Exit

Configuración portchannel 1 D1

Interface range G1/0/5-6

Switchport mode trunk

channel-protocol LACP

channel-group 1 mode activeno

shutdown

exit

validación EtherChannel creados en D1

Comando: show Etherchannel

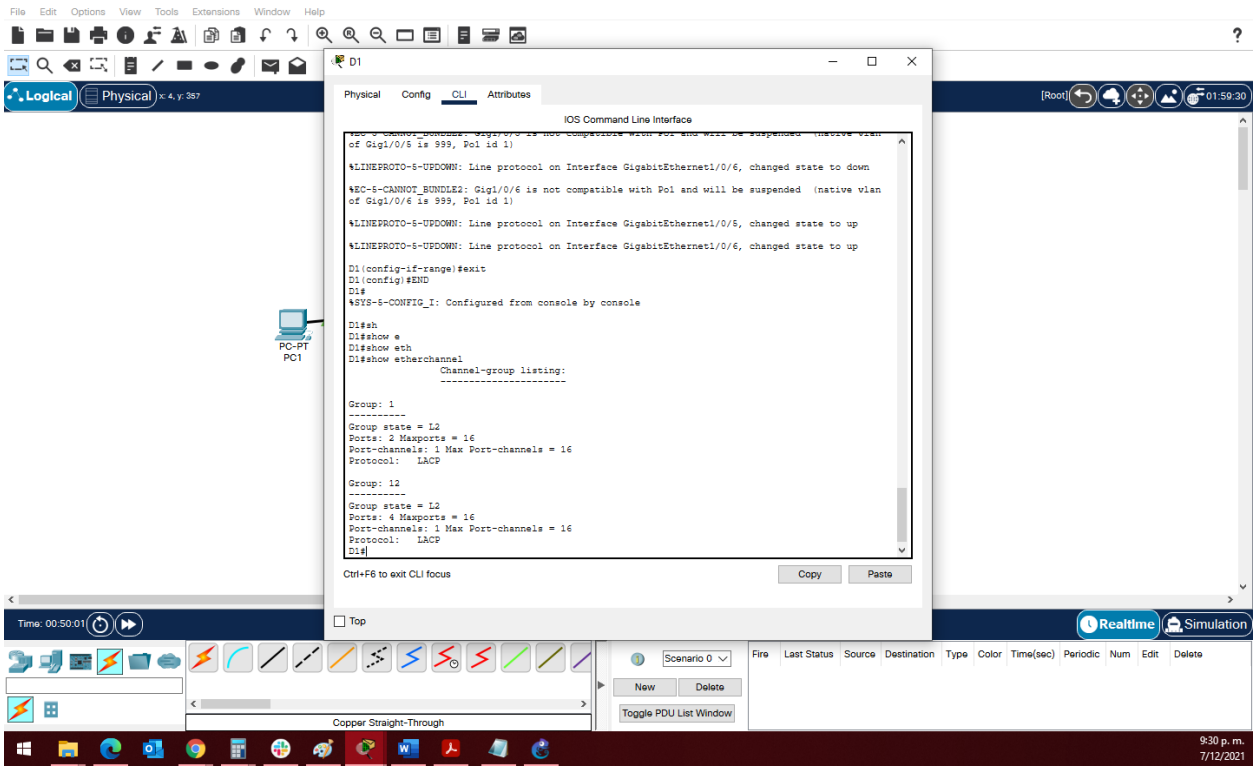


Figura 17Parte2 validación EtherChannel en D1

Creacion PortChannel #12 y #2 en switch D2

Configuración port channel 12 en D2

Config t

interface range G1/0/1-4

channel-protocol LACP

channel-group 12 mode passive

no shutdown

exit

Configuración portchannel 2 D2

Interface range G1/0/5-6

Switchport mode trunk

channel-protocol LACP

channel-group 2 mode active

no shutdown

exit

Validación EtherChannel creados en D2

Comando: show EtherChannel

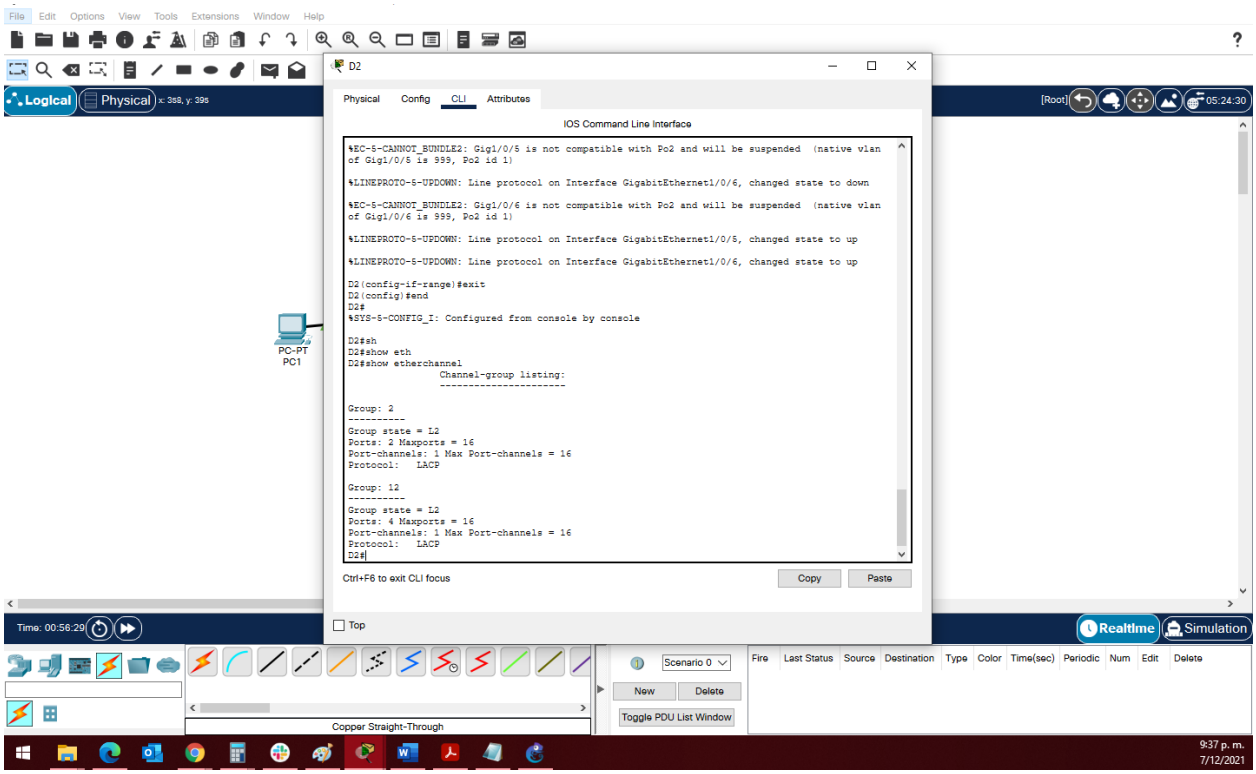


Figura 18 Parte2 validación EtherChannel en D2

Creacion PortChannel #1 y #2 en switch A1

Configuración portchannel 1 A1

Interface range F0/1-2

Switchport mode trunk

channel-protocol LACP

channel-group 1 mode passive

no shutdown

exit

Configuración portchannel 2 A1

Interface range F0/3-4

Switchport mode trunk

channel-protocol LACP

channel-group 2 mode passive

no shutdown

exit

Validación Etherchannels creados en A1

Comando: show EtherChannel

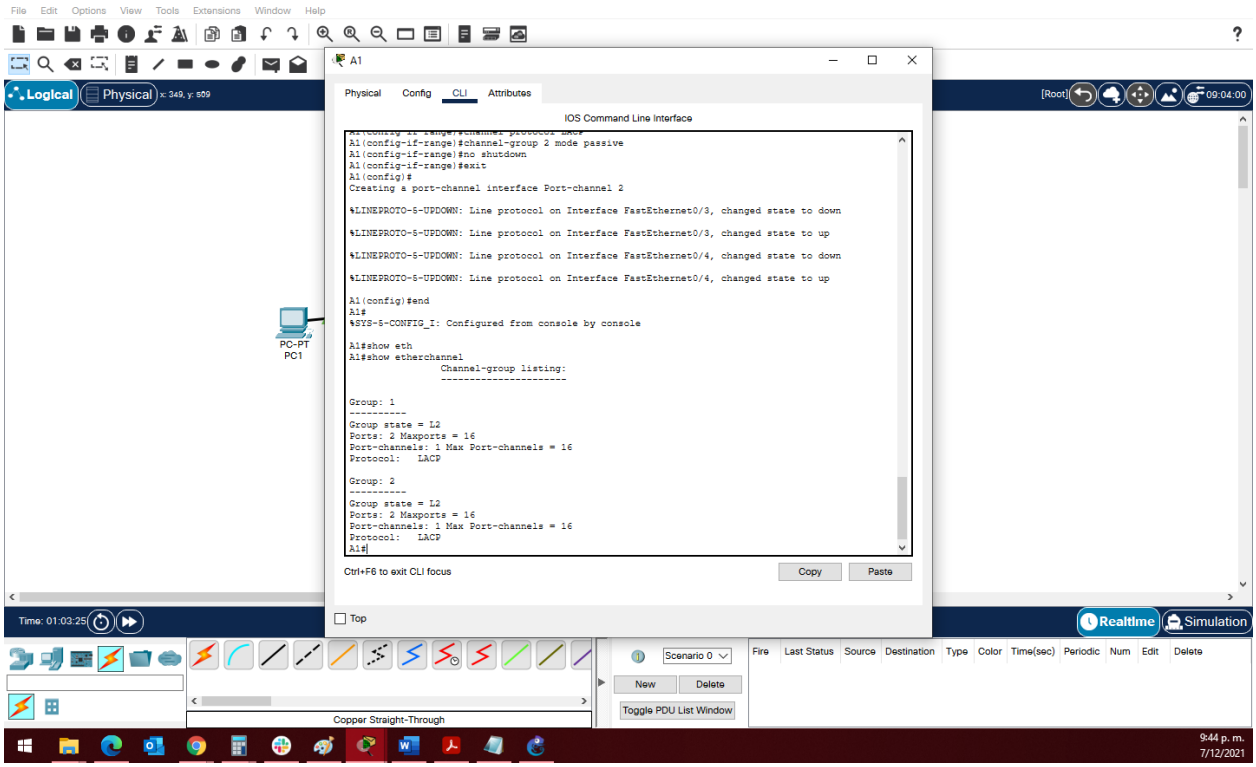


Figura 19 Parte2 validación EtherChannel en D2

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.

Se realiza configuración de puertos de acceso para las conexiones que tienen comoequipo final dispositivos PC dando permisos de acceso por medio de las vlan correspondientes, de igual forma por medio del comando spanning-tree portfast sepermite acceso directo a la red de capa 2 a los equipos finales desde el estado forwarding.

Comandos utilizados en D1

Enable
Config t

interface G1/0/23 switchport
mode access

switchport access vlan 100
spanning-tree portfast

no shutdown

exit

Comandos utilizados en D2

Enable
Config t

interface G1/0/23 switchport
mode access

switchport access vlan 102
spanning-tree portfast

no shutdown

exit

Comandos utilizados en A1

Enable
Config t

interface F0/23 switchport mode
access

switchport access vlan 101
spanning-tree portfast

no shutdown

exit

interface F0/24 switchport mode
access

switchport access vlan 100
spanning-tree portfast

no shutdown

exit

2.7 <u>Verifique los servicios DHCP IPv4.</u>

Se realizará la validación de los PC2 y PC3 donde deberán recibir las direcciones por DHCP en IPV4 validas

Validación de correcto direccionamiento Dhcp desde PC2

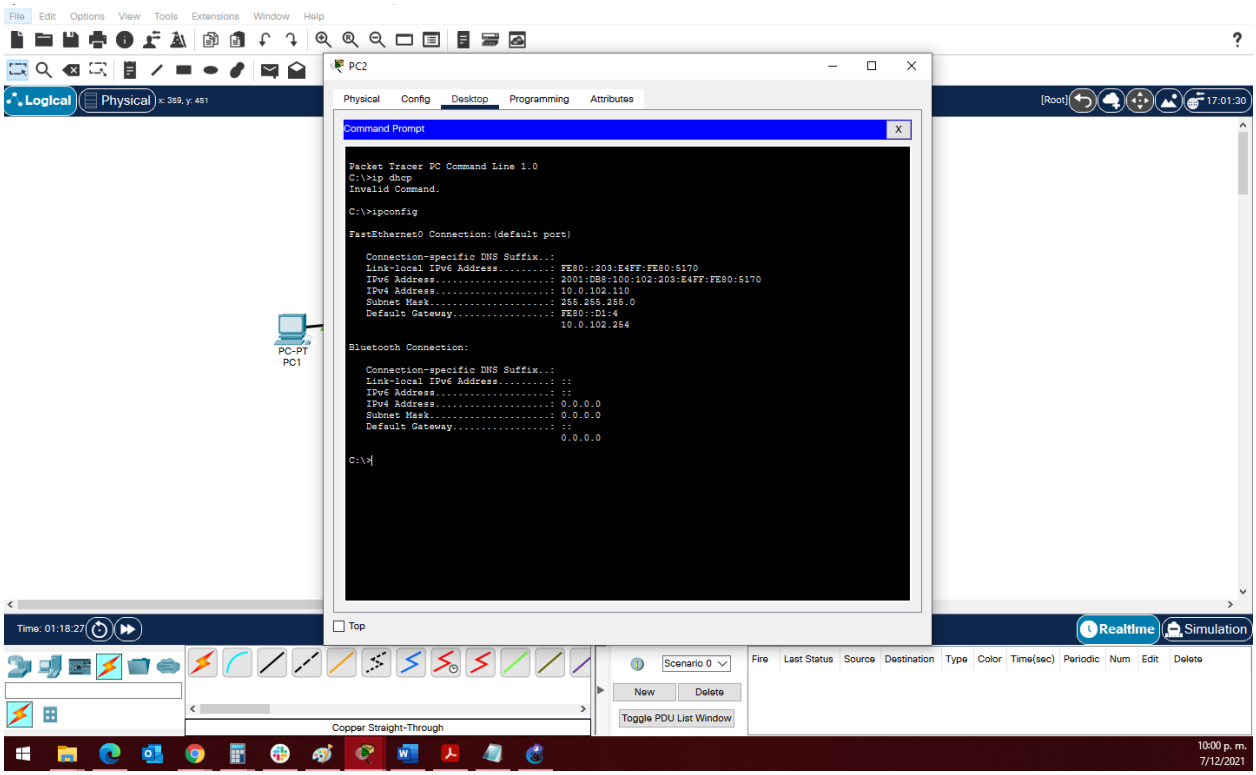


Figura 20 Parte2 Validación DHCP PC2

Validación de correcto direccionamiento Dhcp desde PC3

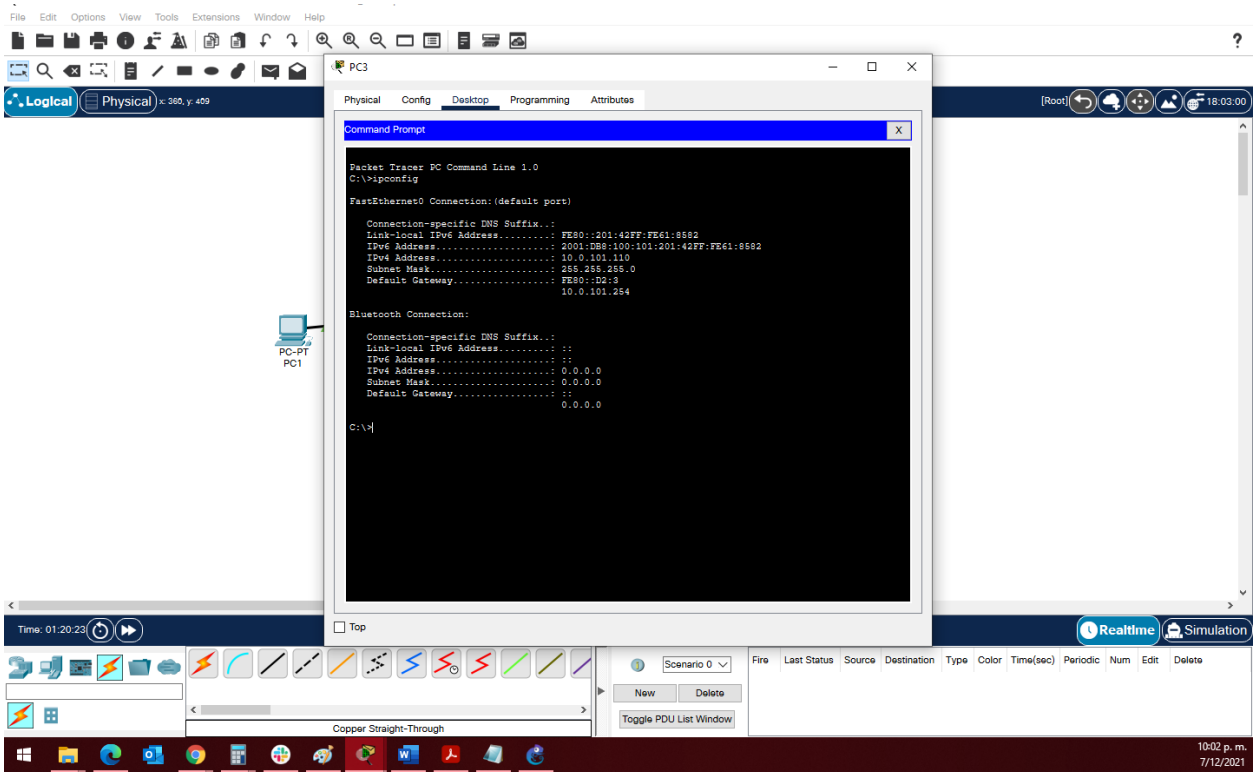


Figura 21 Parte2 Validación DHCP PC3

2.8 Verifique la conectividad de la LAN local

Se realiza por medio del comando ping la validación de conexión de punto a punto donde nos permitirá visualizar su envió y recepción exitosamente

Validaciones de conectividad desde PC1

Ping hacia D1 IP 10.0.100.1

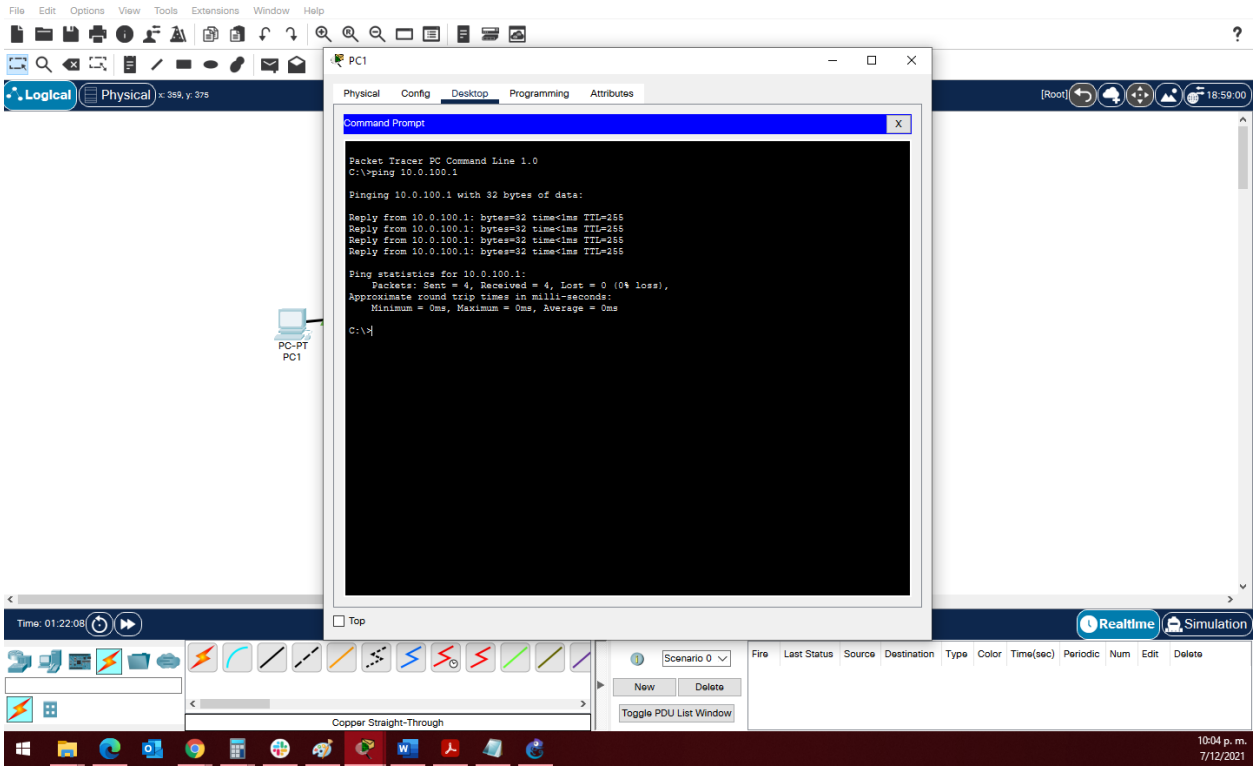


Figura 22 Parte2 Conectividad LAN PC1 D1

Ping hacia D2 IP 10.0.100.2

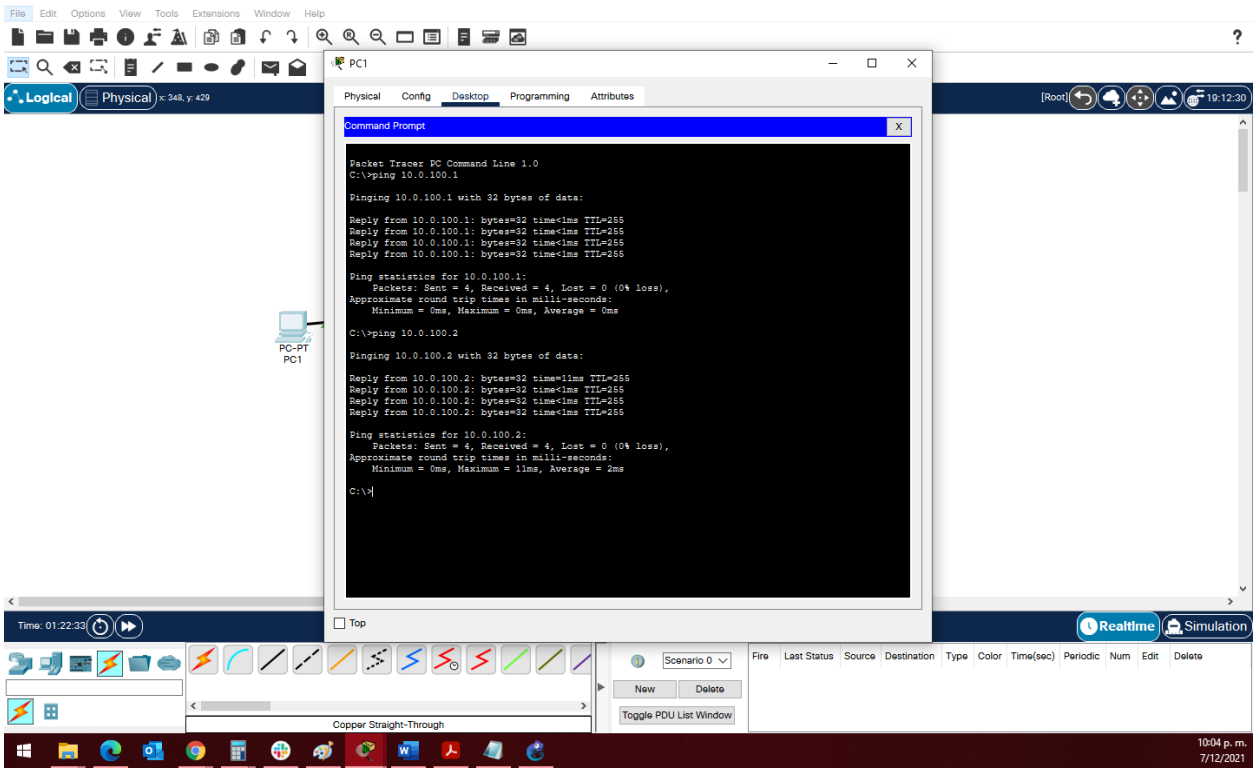


Figura 23 Parte2 Conectividad LAN PC1 hacia D2

Ping hacia PC4 IP 10.0.100.6

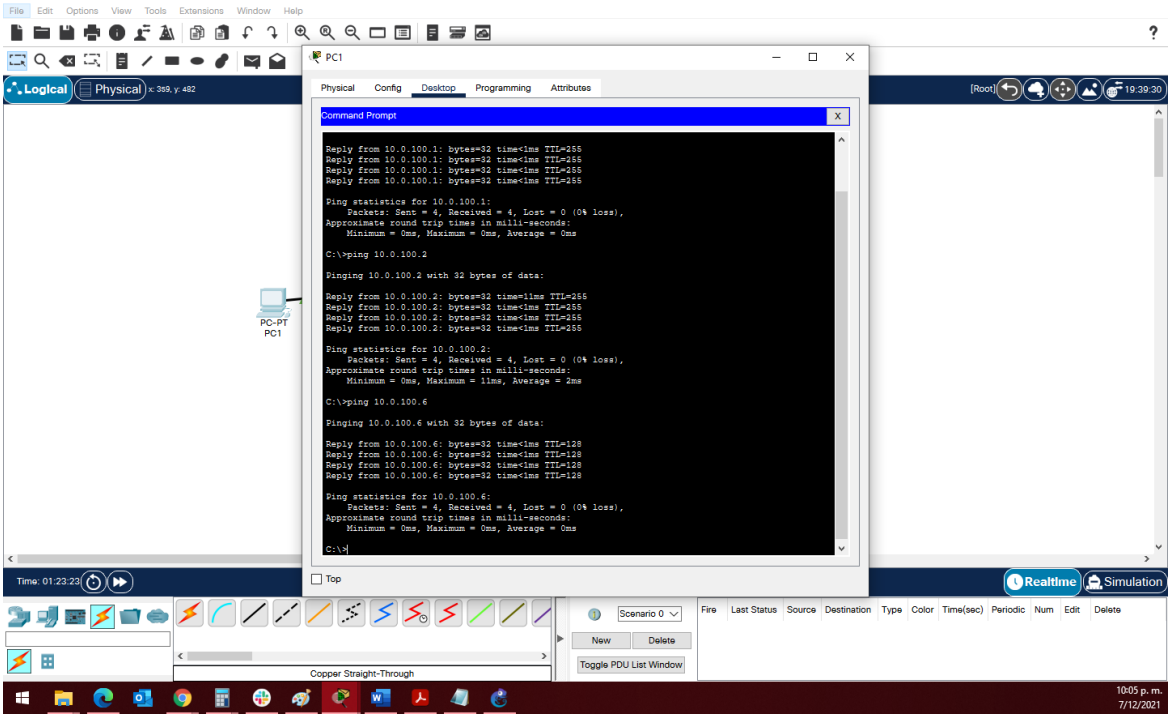


Figura 24 Parte2 Conectividad LAN PC1 hacia PC4

Validaciones de conectividad desde PC2

Ping hacia D1 IP 10.0.102.1

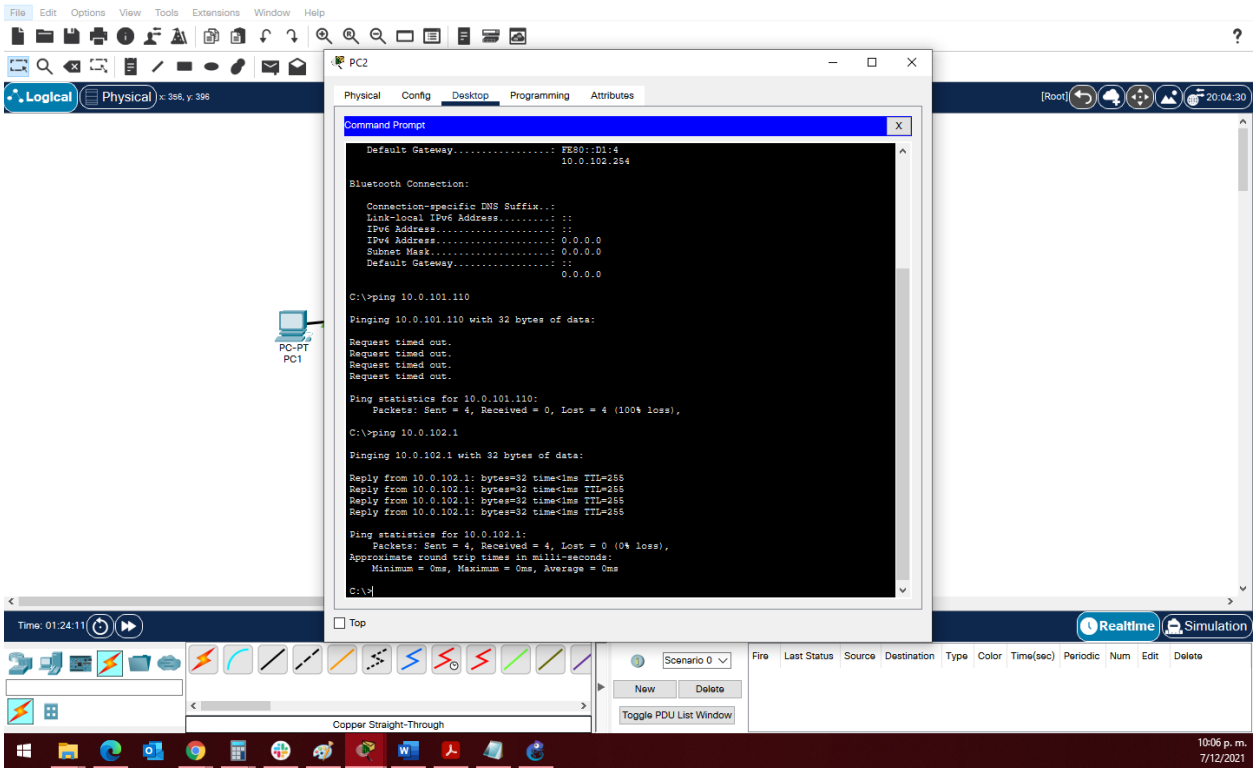


Figura 25 Parte2 Conectividad LAN PC2 hacia D1

Ping hacia D2 IP 10.0.102.2

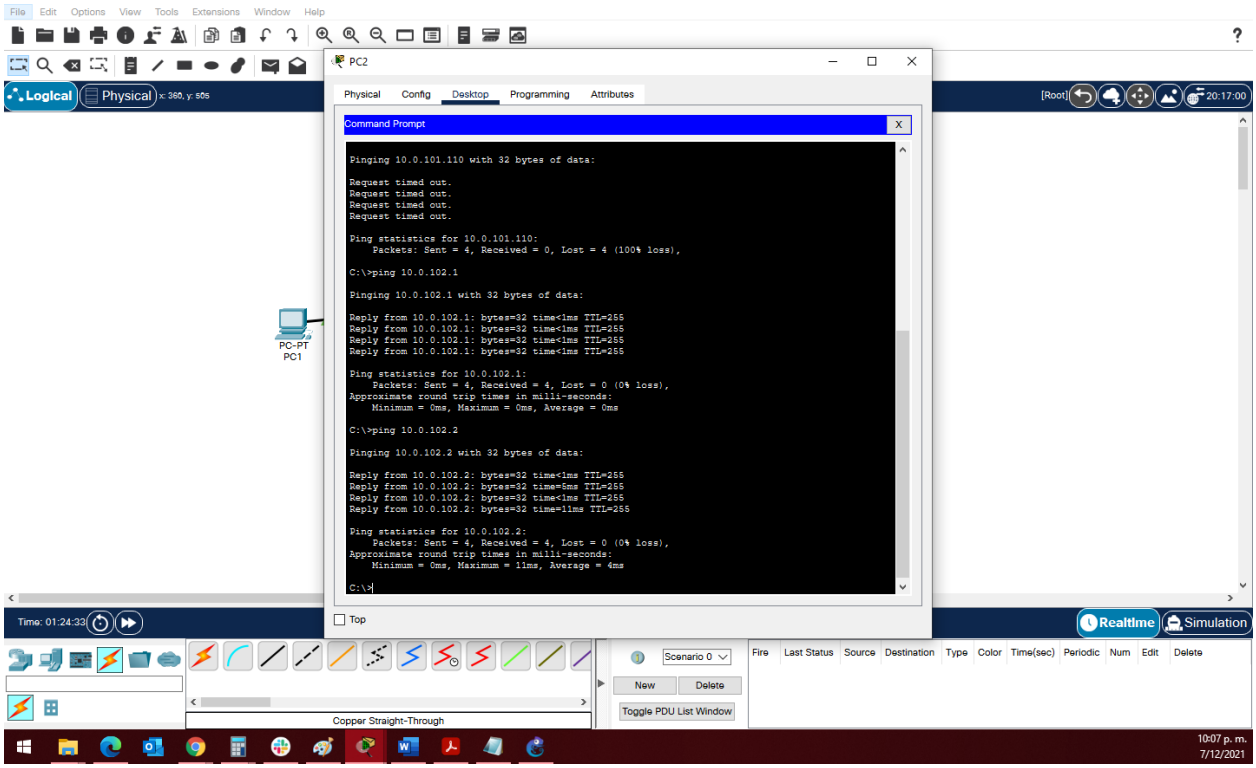


Figura 26 Parte2 Conectividad LAN PC2 hacia D2

Validaciones de conectividad desde PC3

Ping hacia D1 IP 10.0.101.1

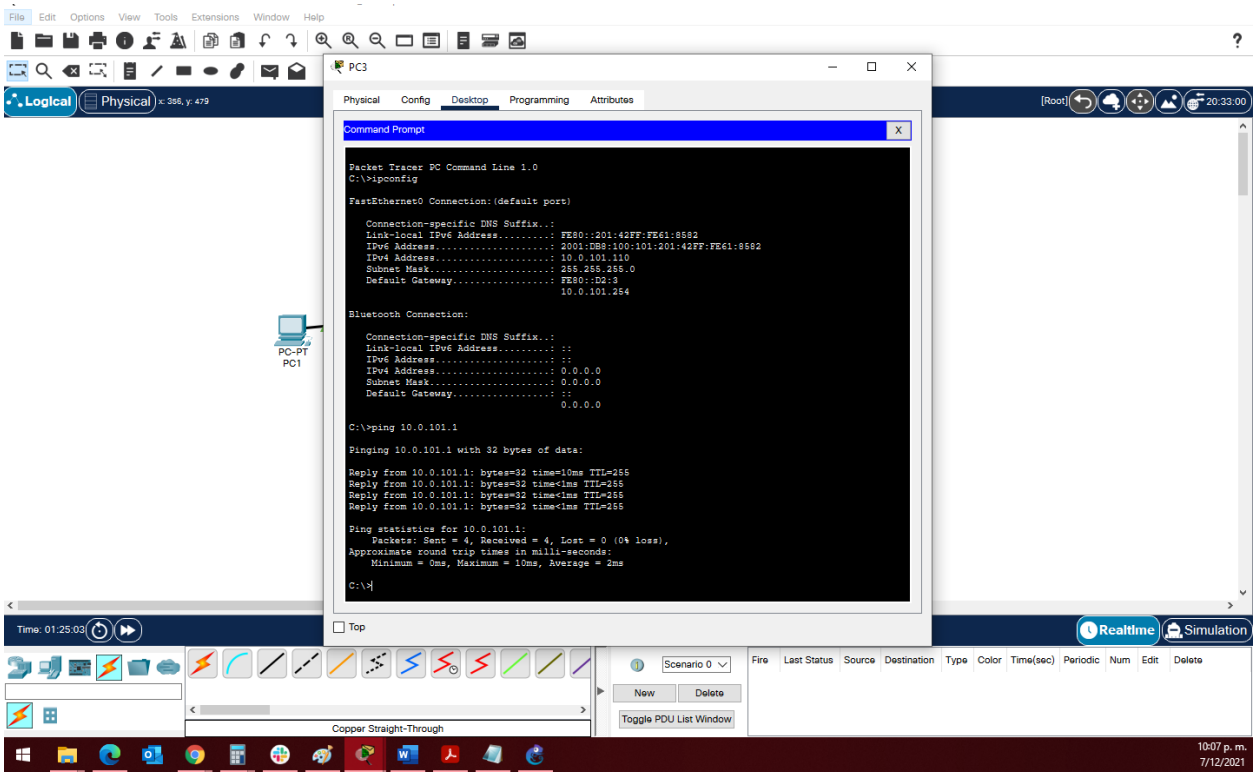


Figura 27 Parte2 Conectividad LAN PC3 hacia D1

Ping hacia D2 IP 10.0.101.2

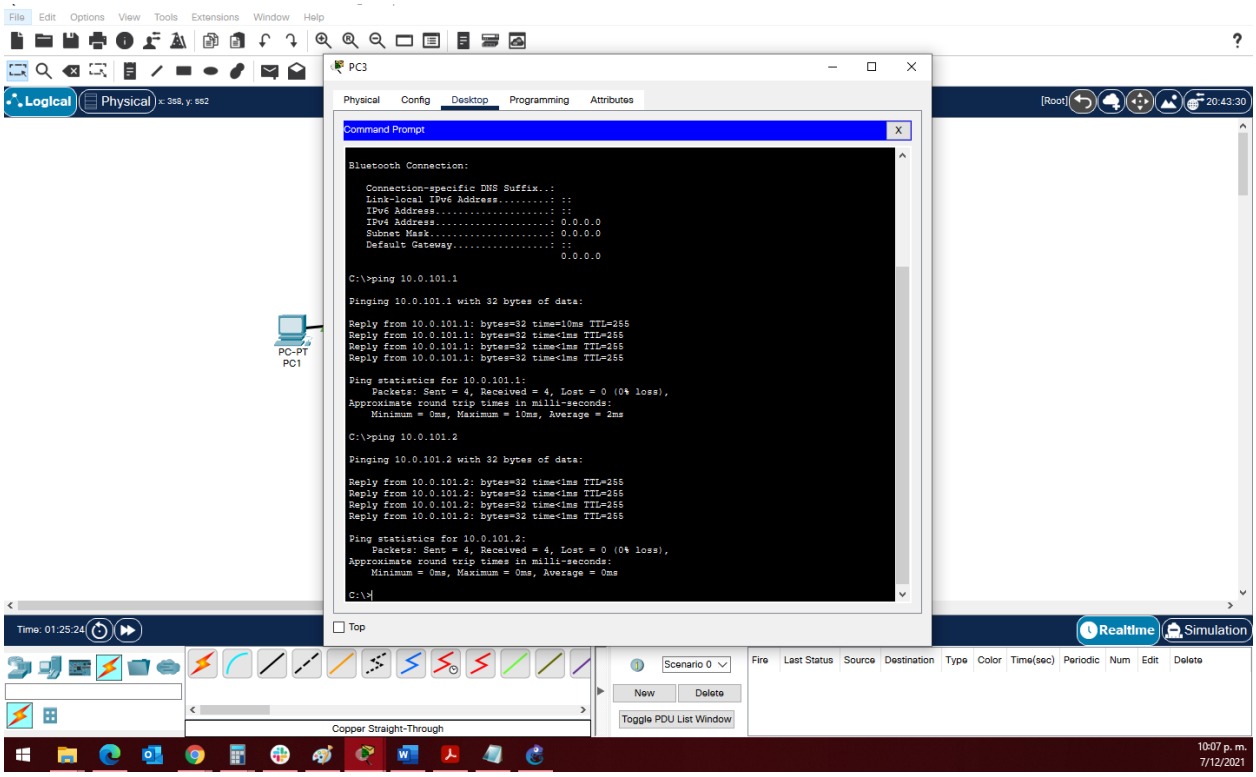


Figura 28 Parte2 Conectividad LAN PC3 hacia D2

Validaciones de conectividad desde PC4

Ping hacia D1 IP 10.0.100.1

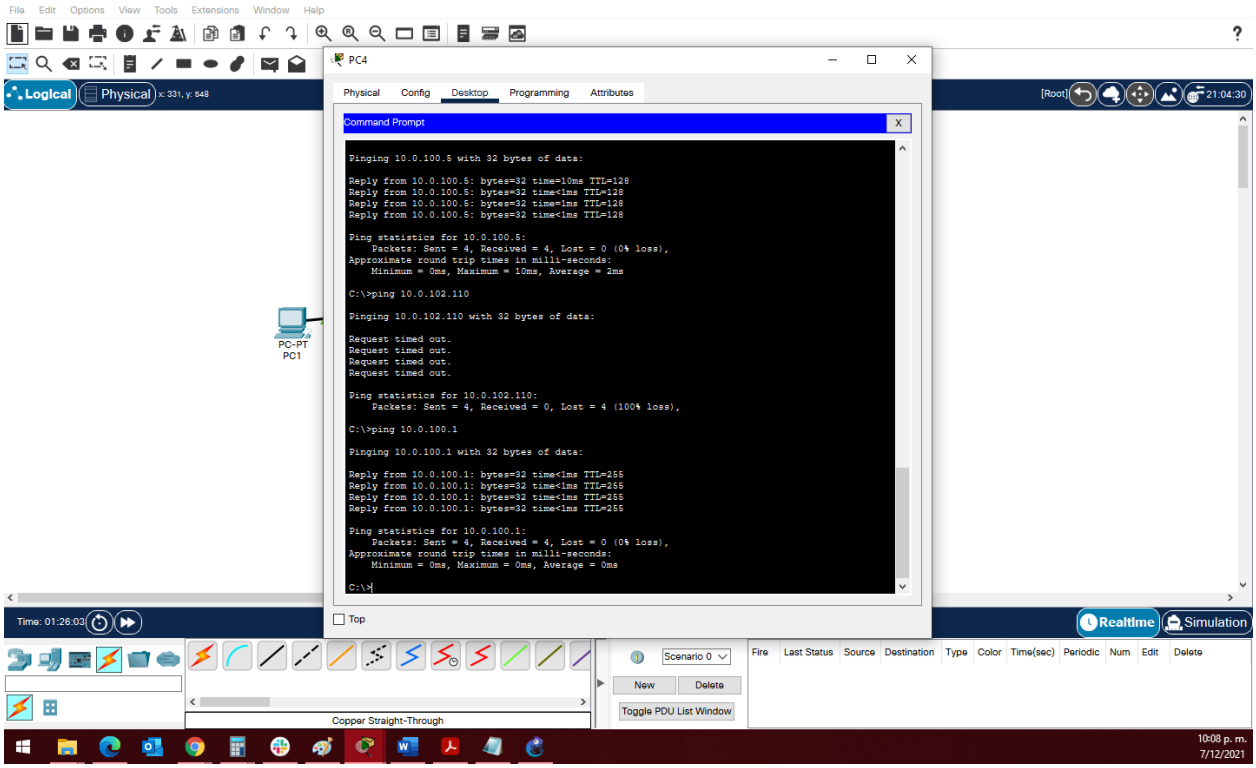


Figura 29 Parte2 Conectividad LAN PC4 hacia D1

Ping hacia D2 IP 10.0.100.2

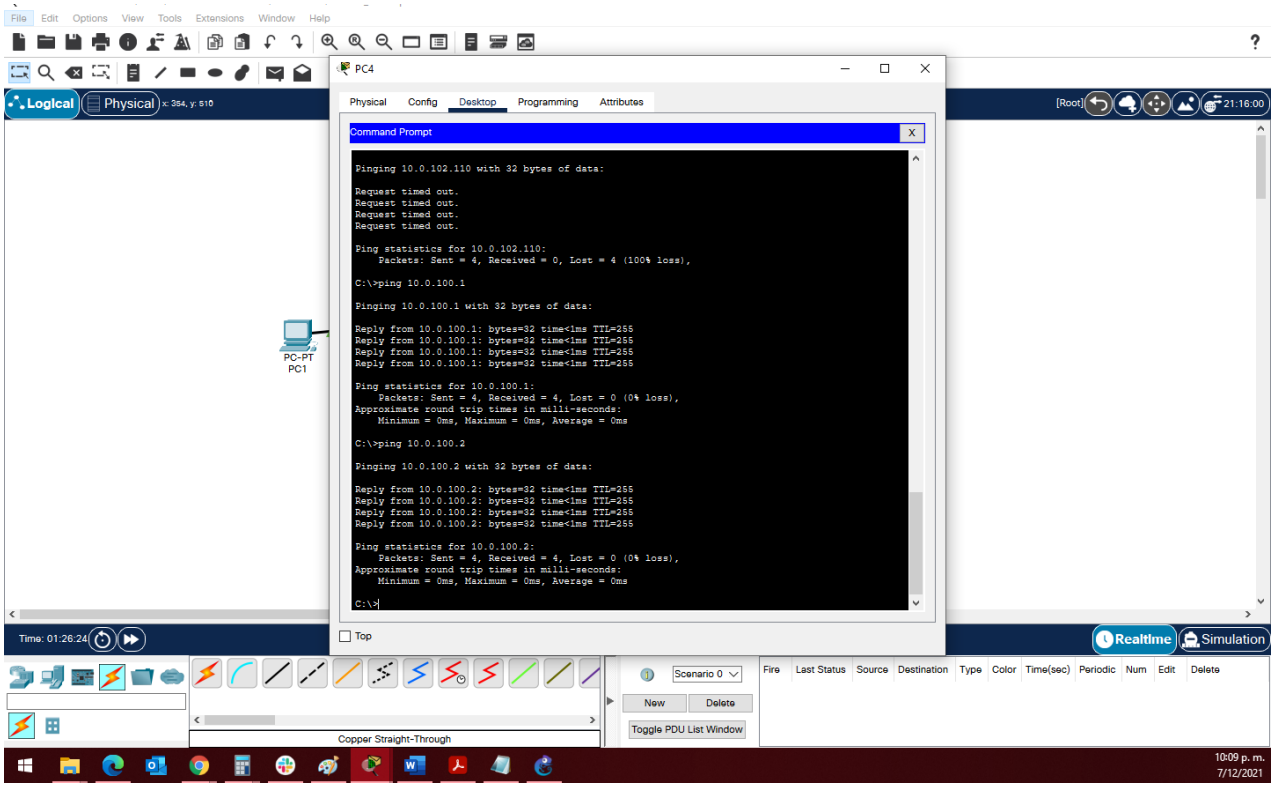


Figura 30 Parte2 Conectividad LAN PC4 hacia D2

Ping hacia PC1 IP 10.0.100.5

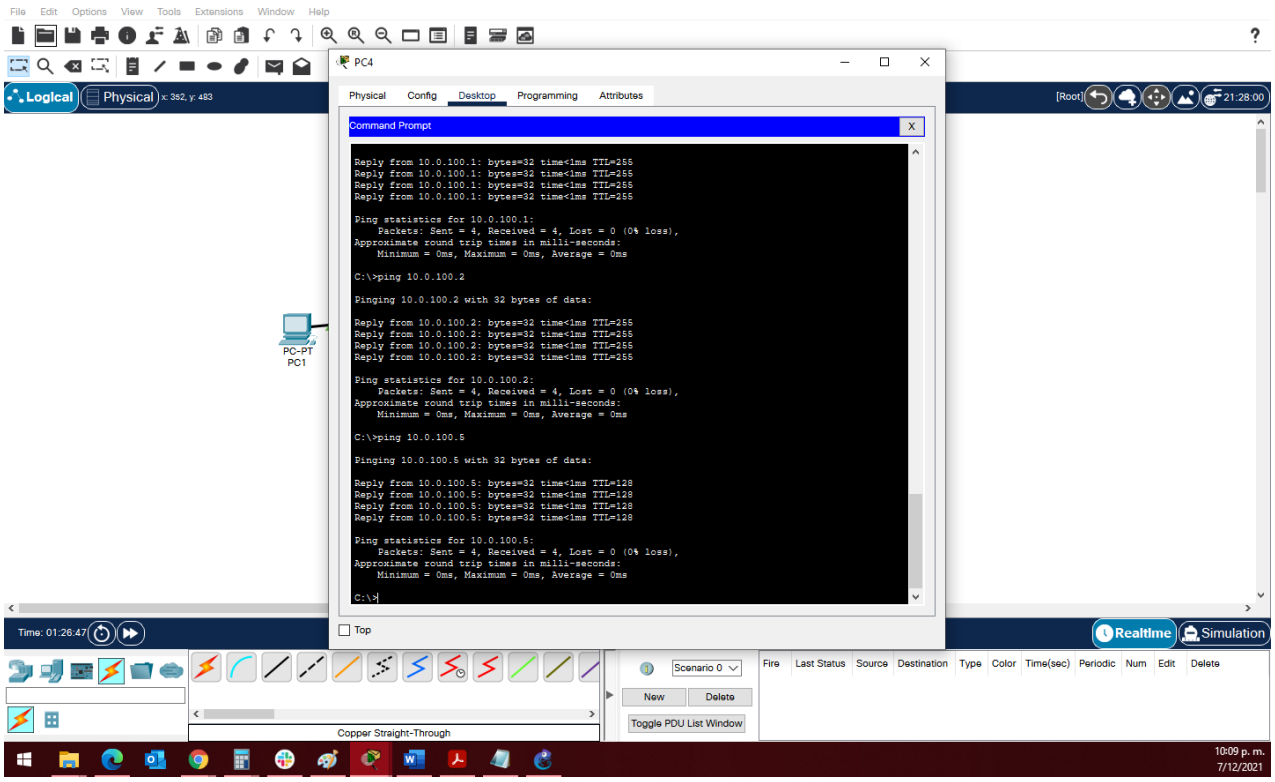


Figura 31 Parte2 Conectividad LAN PC4 hacia PC1

Parte 3: Configurar los protocolos de enrutamiento

En esta grandiosa parte (3.1, 3.2, 3.3 y 3.4) se configurará los protocolos IPV4 e IPV6 donde al final la red deberá estar completamente convergente, se validará con el comando ping los protocolos ya dichos donde deberá haber conexión exitosa con la interfaz Loopback 0 desde D1 y D2. Cabe indicar que el ping de conexión no será exitoso ya que las puertas de enlace ya predeterminadas van hacia la network HSRP donde se habilitara en la parte 4.

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

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: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1. 0.0.4.131 • D2. 0.0.4.132 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

Figura 32 Configuración a realizar en parte 3 punto 3.1

Configuración en Router R1

Anunciación de las VLAN en Router R1

```
R1>enable
```

```
R1#config terminal
R1(config)#interface g0/0/1.100

R1(config-subif)#encapsulation dot1Q 100
```

```
R1(config-subif)#ip address 10.0.100.1 255.255.255.0
R1(config-subif)#exit

R1(config)#interface g0/0/1.101
R1(config-subif)#encapsulation dot1Q 101
R1(config-subif)#ip address 10.0.101.1 255.255.255.0
R1(config-subif)#exit

R1(config)#interface g0/0/1.102
R1(config-subif)#encapsulation dot1Q 102
R1(config-subif)#ip address 10.0.102.1 255.255.255.0
R1(config-subif)#exit
```

Configuración de OSPF en R1

```
R1#config terminal
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
```

Anunciación de las redes conectadas a R1 con las VLANS

```
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)#network 10.0.100.0 0.0.0.255 area 0
R1(config-router)#network 10.0.101.0 0.0.0.255 area 0
R1(config-router)#network 10.0.102.0 0.0.0.255 area 0
R1(config-router)#exit
```

propagación de ruta por defecto en R1

R1#CONFIG Terminal R1(config)#router
ospf 4

R1(config-router)#default-information originate
R1(config-router)#exit

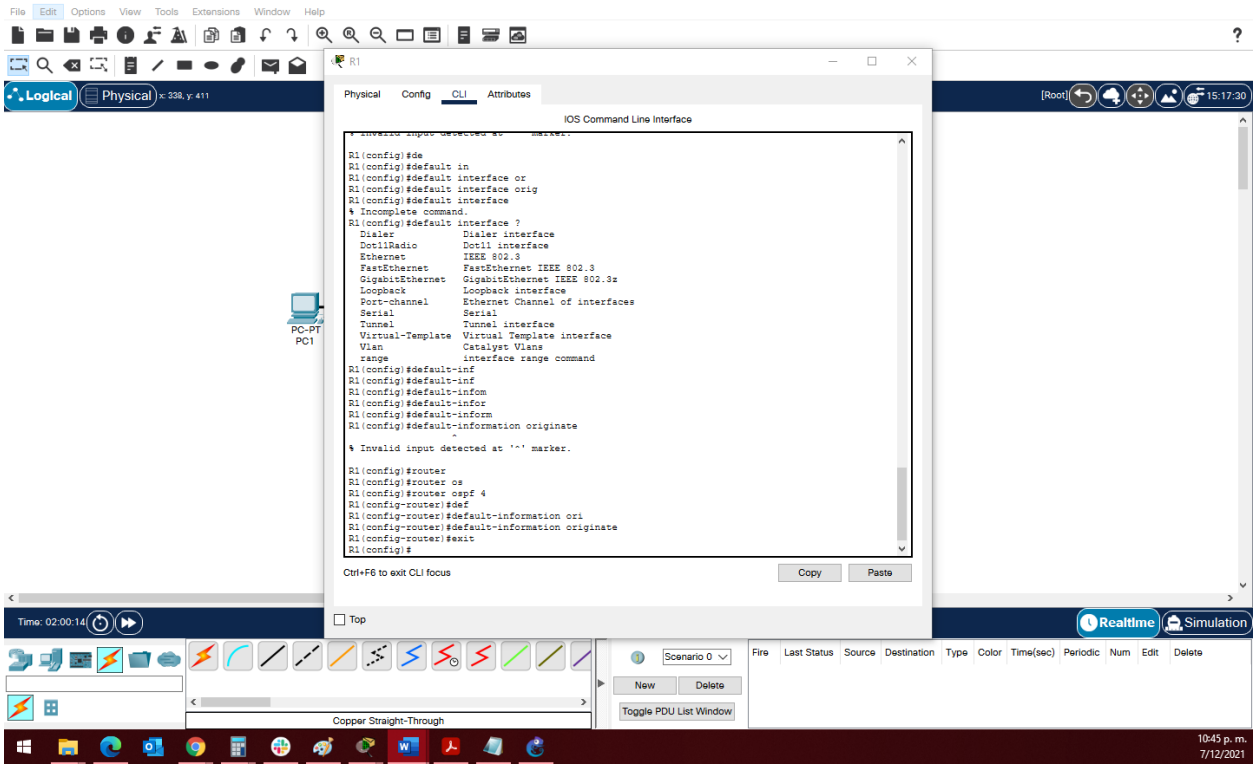


Figura 33 Validación configuración OSPF R 1

Configuración en Router R3

R3>enable

R3#config terminal
R3(config)#interface g0/0/1.100

R3(config-subif)#encapsulation dot1Q 100

R3(config-subif)#ip address 10.0.100.2 255.255.255.0

R3(config-subif)#exit

R3(config)#interface g0/0/1.101

-subif)#encapsulation dot1Q 101

R3(config-subif)#ip address 10.0.101.2 255.255.255.0
R3(config-subif)#exit

R3(config)#interface g0/0/1.102

R3(config-subif)#encapsulation dot1Q 102

R3(config-subif)#ip address 10.0.102.2 255.255.255.0

R3(config-subif)#exit

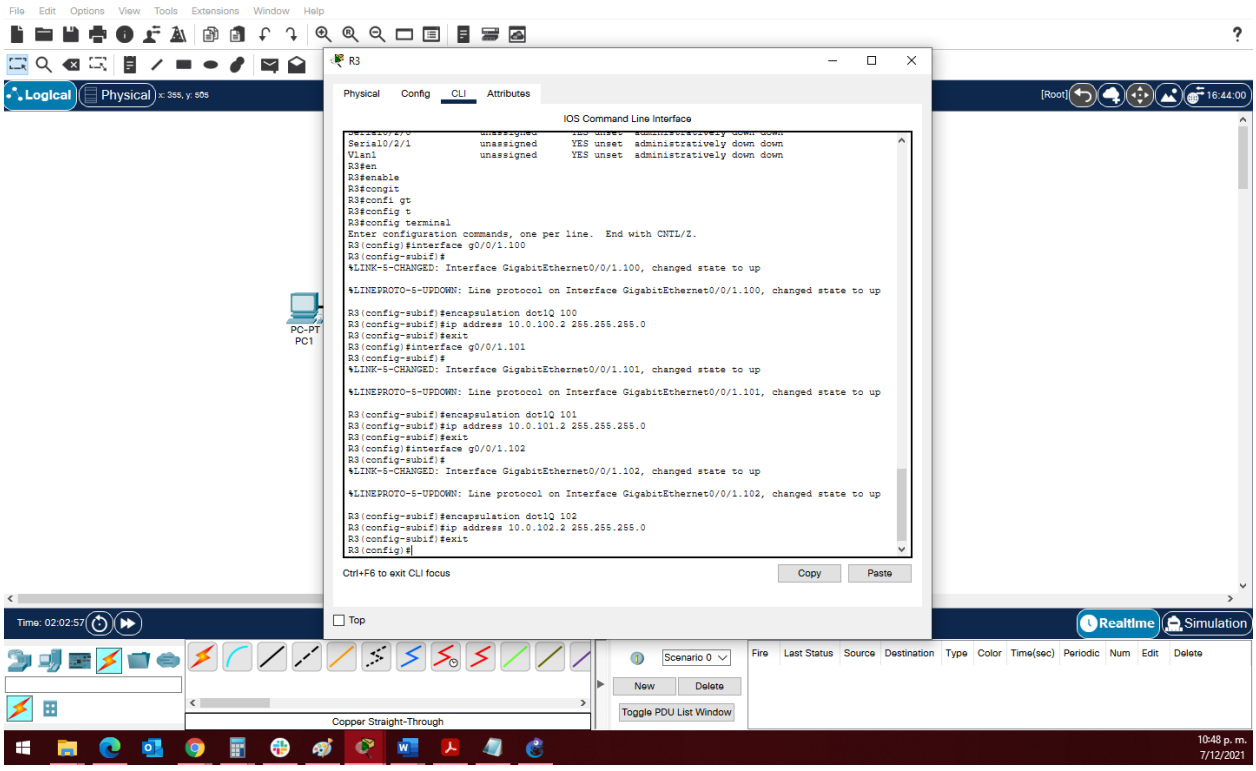


Figura 34 Anunciación de las VLAN en Router R3

Aplicación de comando show ip route en R1 y R3

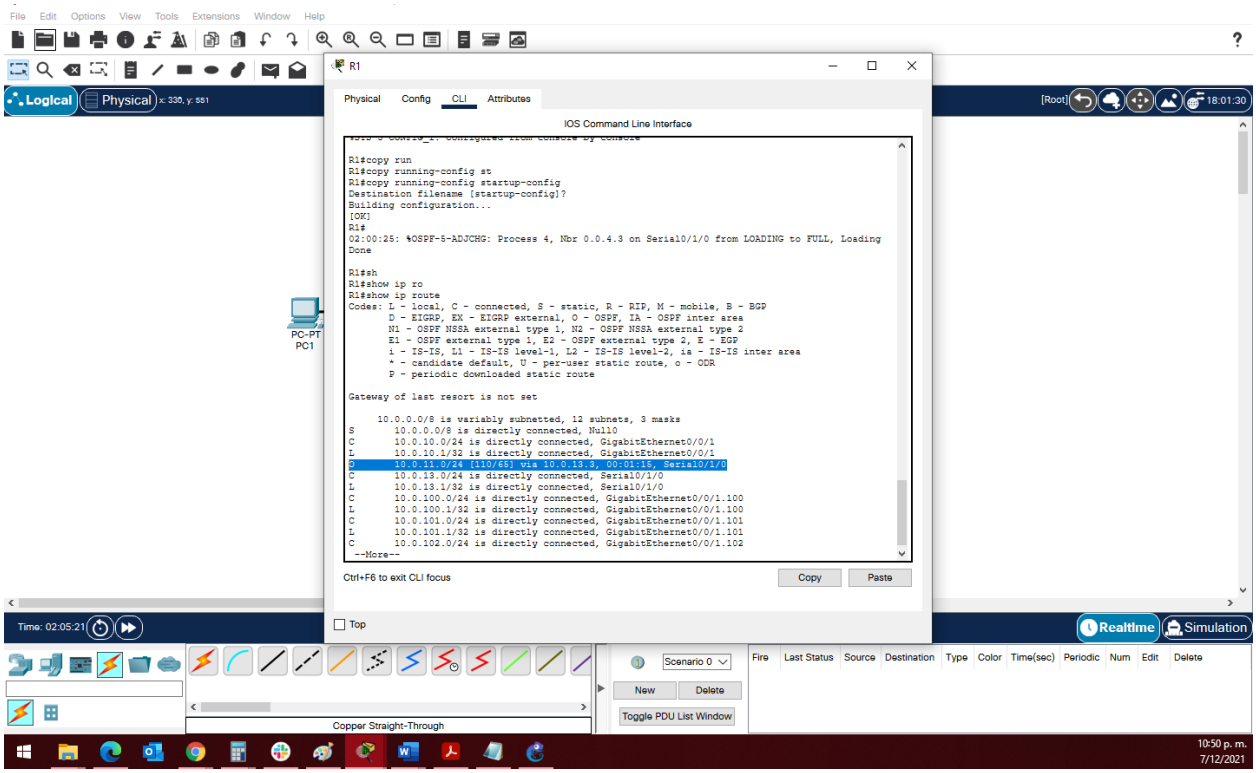


Figura 35 Visualización de protocolo OSPF activo en R1

Aplicación de comando show ip route en R1 y R3

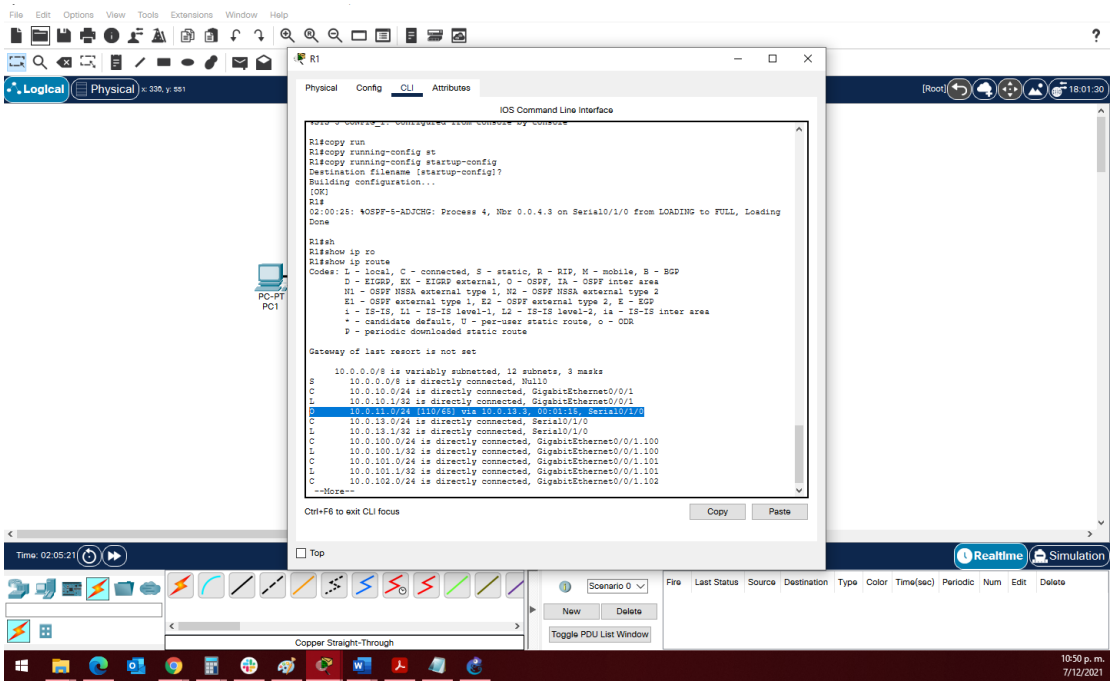


Figura 36 Visualización de protocolo OSPF activo en R1

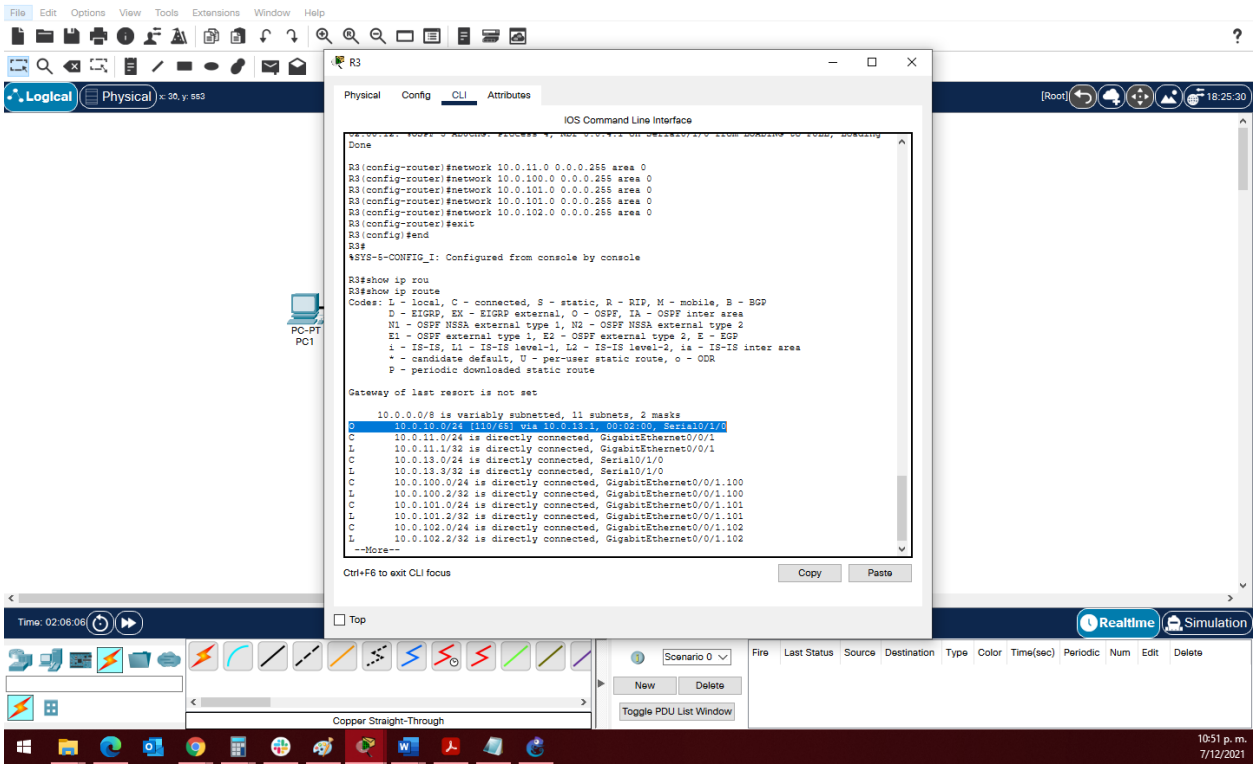


Figura 37 Visualización de protocolo OSPF activo en R3

Configuración en SWITCH D1

Configuración de OSPF en D1

D1(config)#router ospf 4

D1(config-router)#router-id 0.0.4.131

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

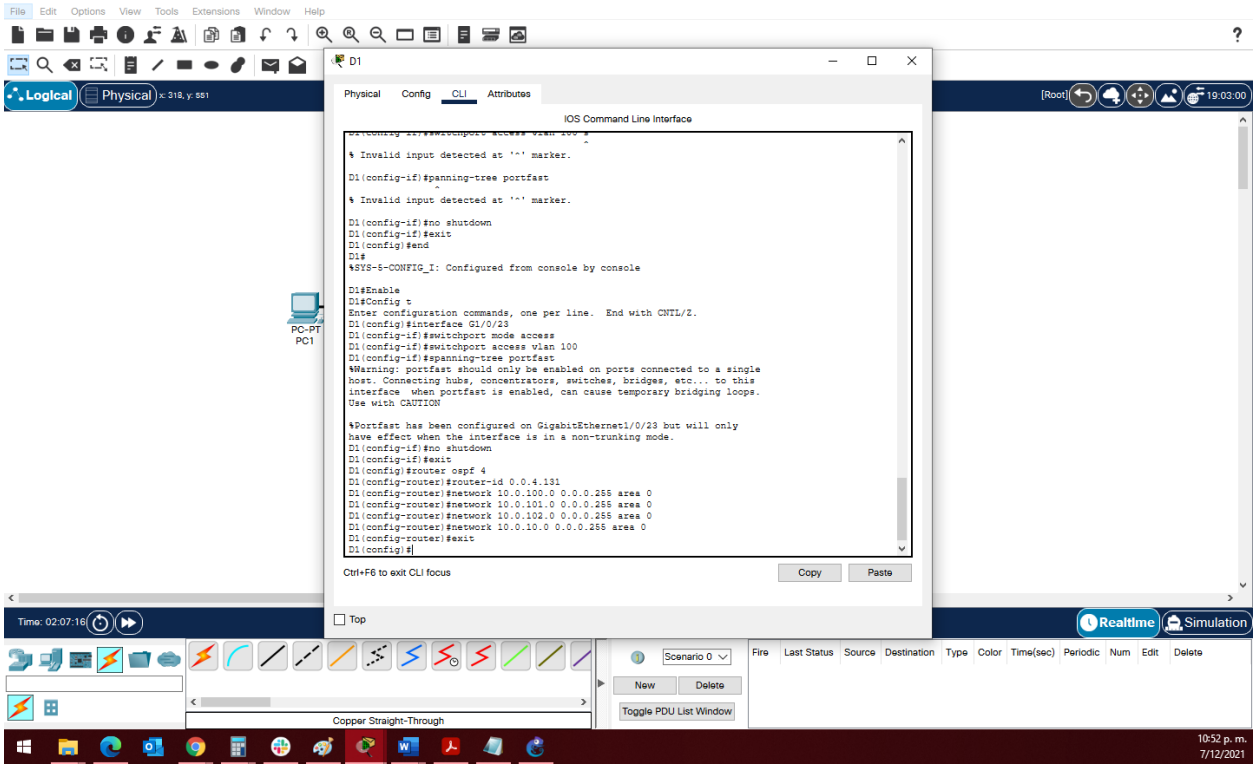


Figura 38 Configuración de OSPF en D1

Configuración en SWITCH D2

Configuración de OSPF en D2

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
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
```

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

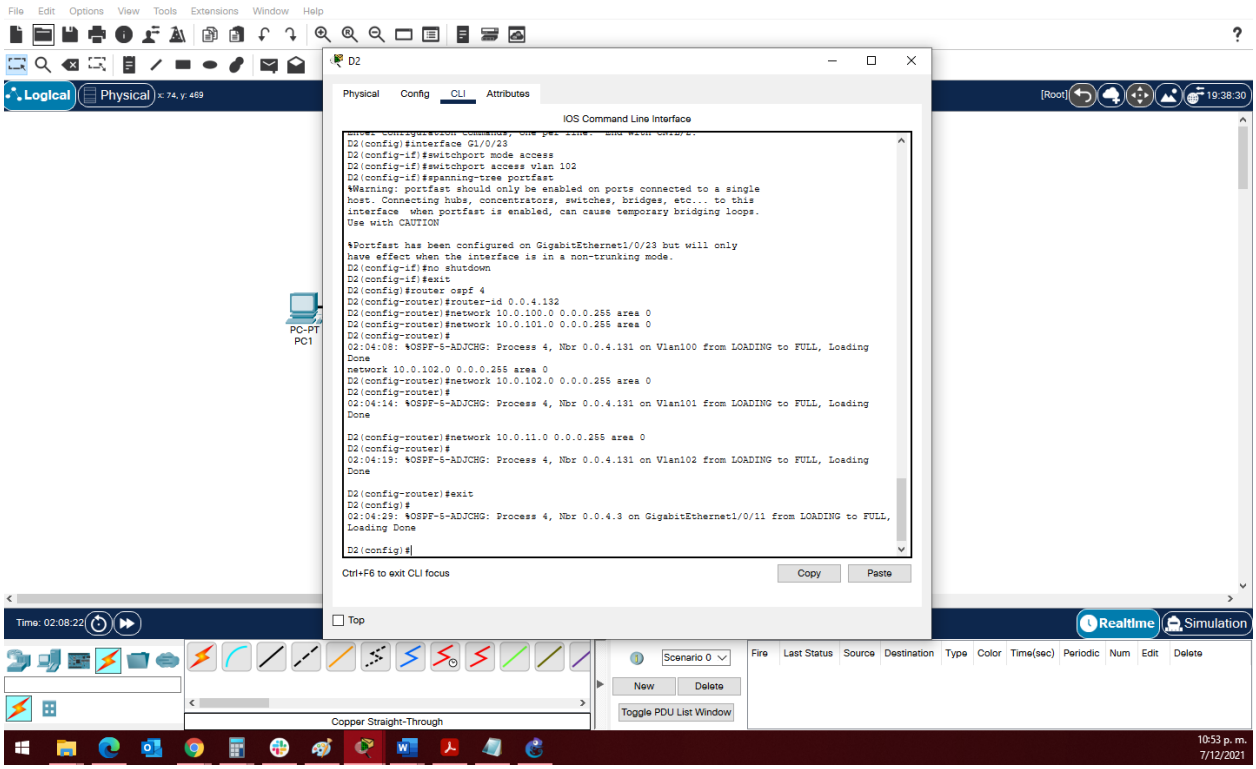


Figura 39 Configuración de OSPF en D2

Aplicamos de nuevo el comando show ip route

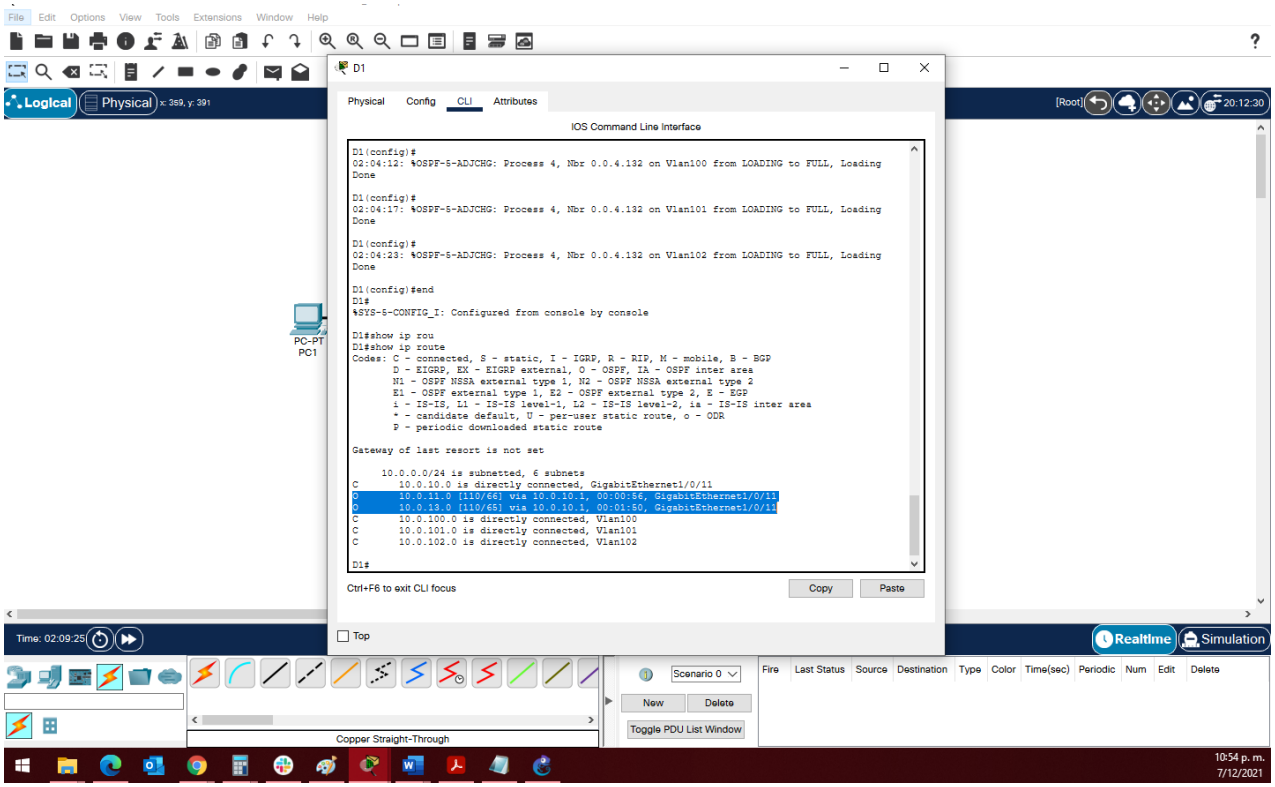


Figura 40 Visualización de protocolo OSPF activo en D1

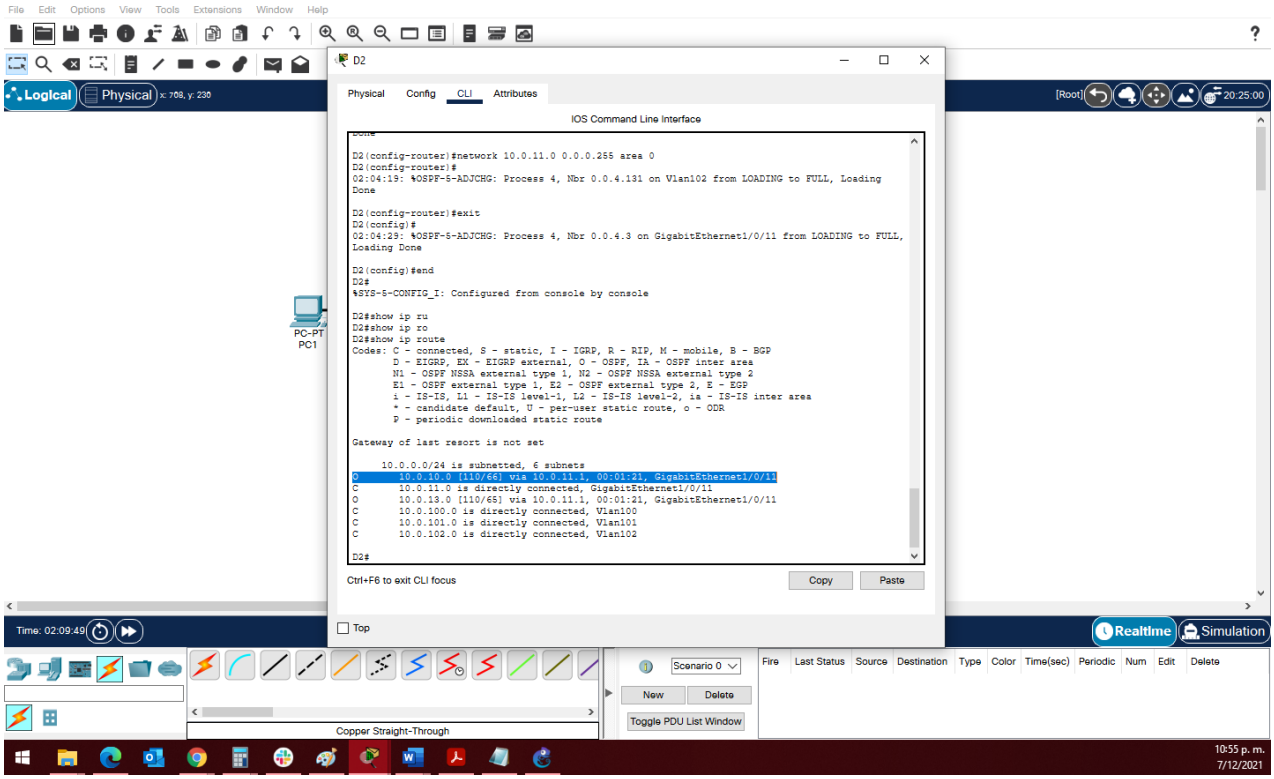


Figura 41 Visualización de protocolo OSPF activo en D2

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

3.2	En la "Red de la Compañia" (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: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • 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. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

Figura 42 Configuración a realizar en parte 3 punto 3.2

Router R1 configuración para recibir IPV6 y protocolo OSPFv3

R1#config te

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing

R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#

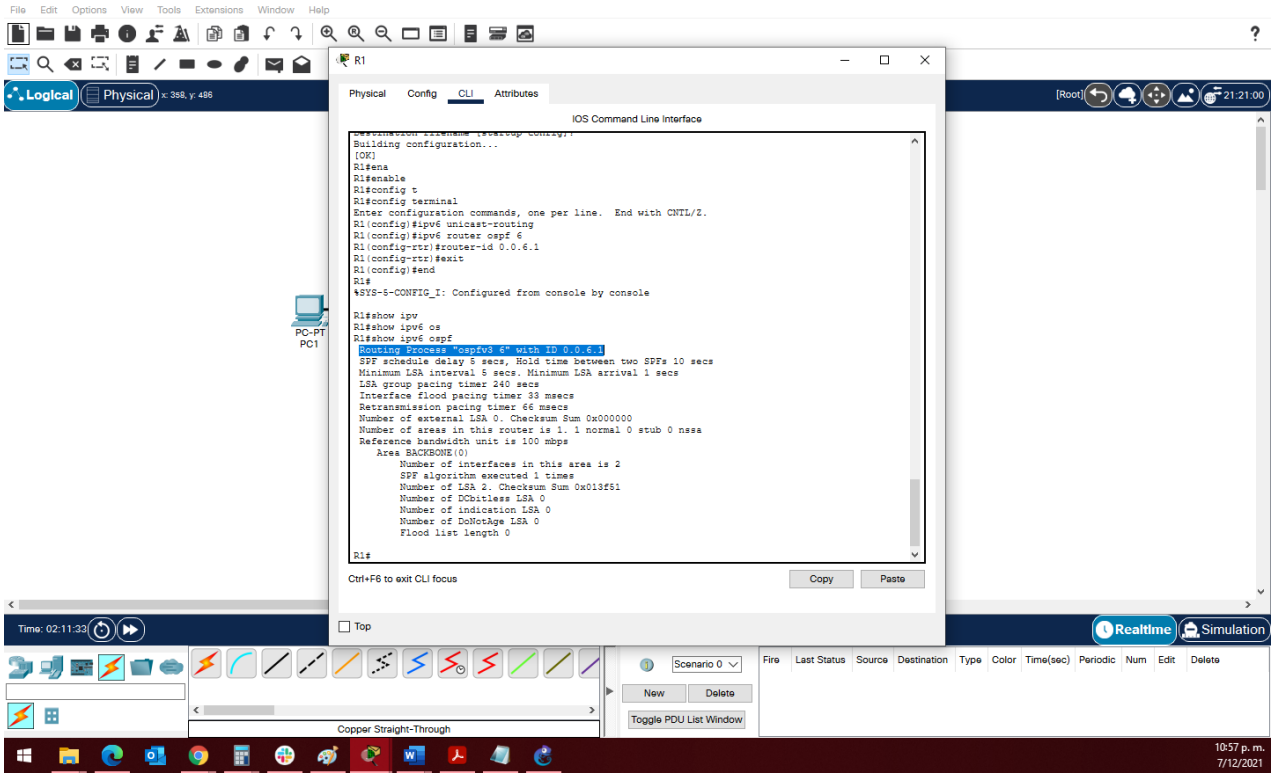


Figura 43 Visualización OSPFv3 Activo

Anunciación de las VLAN en R1

R1(config)#interface g0/0/1.100

R1(config-subif)#encapsulation dot1Q 100

R1(config-subif)#ipv6 address 2001:db8:100:100::1/64
R1(config-subif)#exit

R1(config)#interface g0/0/1.101

R1(config-subif)#encapsulation dot1Q 101

R1(config-subif)#ipv6 address 2001:db8:100:101::1/64
R1(config-subif)#exit

R1(config)#interface g0/0/1.102

R1(config-subif)#encapsulation dot1Q 102

R1(config-subif)#ipv6 address 2001:db8:100:102::1/64
R1(config-subif)#exit

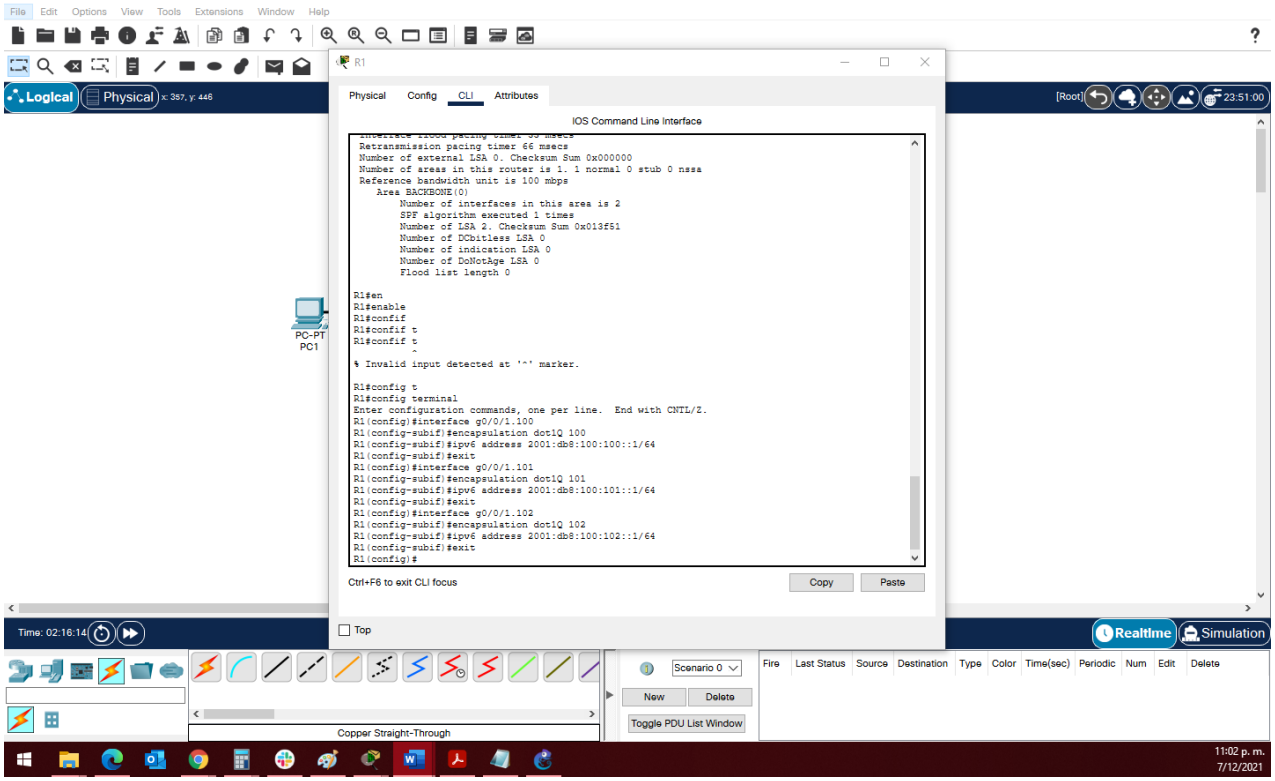


Figura 44 anunciación de las VLAN en R1

Configuración de OSPFV3 en R1

Configuración OSPFv3 por puerto g0/0/1

R1#CONFIG TERM

```
R1(config)#interface g0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
```

Configuración OSPFv3 por puerto s0/1/0

```
R1(config)#interface s0/1/0 R1(config-
if)#ipv6 ospf 6 area 0R1(config-if)#exit
```

Configuración OSPFv3 por puerto g0/0/1.100 el cual es el ingreso de la VLAN 100

```
R1(config)#interface g0/0/1.100
R1(config-subif)#ipv6 ospf 6 area 0
R1(config-subif)#exit
```

Configuración OSPFv3 por puerto g0/0/1.101 el cual es el ingreso de la VLAN 101

```
R1(config)#interface g0/0/1.101
R1(config-subif)#ipv6 ospf 6 area 0
R1(config-subif)#exit
```

Configuración OSPFv3 por puerto g0/0/1.102 el cual es el ingreso de la VLAN 102

```
R1(config)#interface g0/0/1.102
R1(config-subif)#ipv6 ospf 6 area 0
R1(config-subif)#exit
```

Propagación de ruta por defecto en R1

R1(config)#ipv6 router ospf 6

R1(config-rtr)#default-information originate
R1(config-rtr)#exit

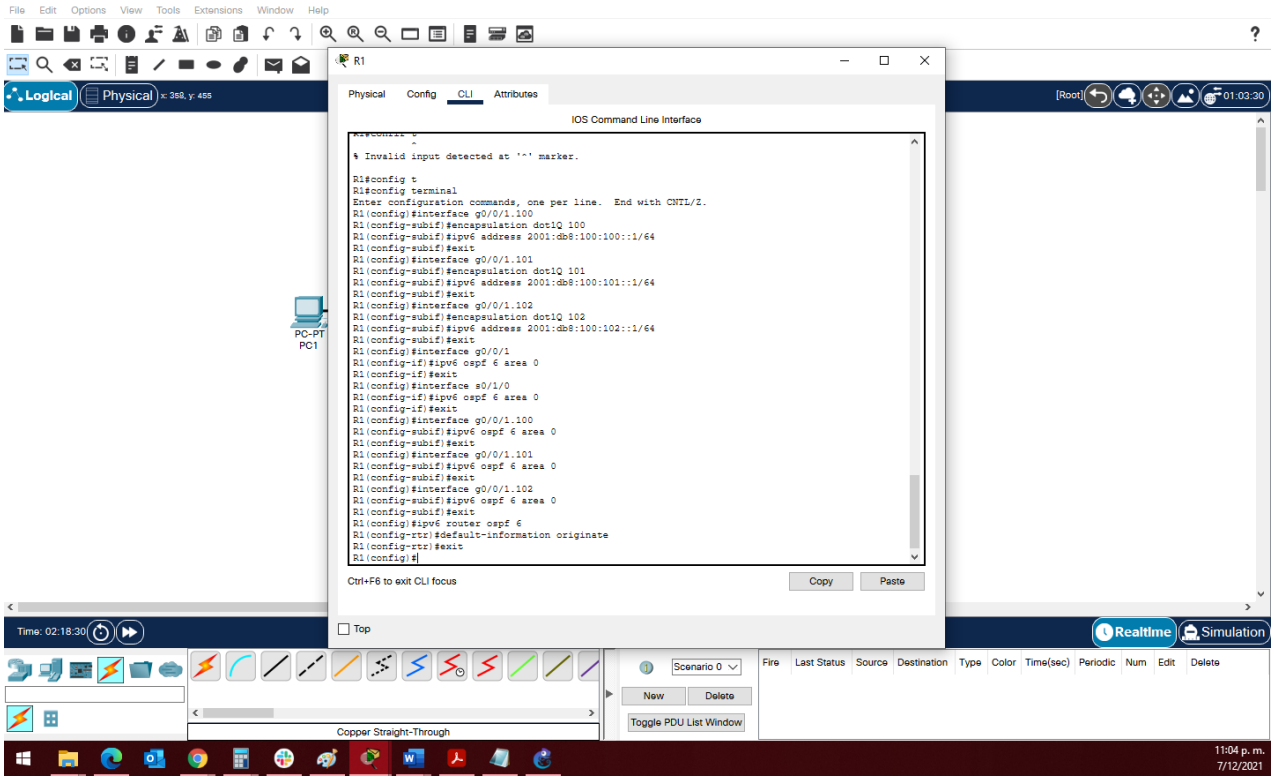


Figura 45 Configuración de OSPFV3 en R1

Configuración R3 para protocolo OSPFV3 y configuración ID

R3#config terminal
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3

Anunciación de las VLAN en R3

R3>enable
R3#config terminal

R3(config)#interface g0/0/1.100

R3(config-subif)#encapsulation dot1Q 100

R3(config-subif)#ipv6 address 2001:db8:100:100::2/64
R3(config-subif)#exit

R3(config)#interface g0/0/1.101

R3(config-subif)#encapsulation dot1Q 101

R3(config-subif)#ipv6 address 2001:db8:100:101::2/64
R3(config-subif)#exit

R3(config)#interface g0/0/1.102

R3(config-subif)#ipv6 address 2001:db8:100:102::2/64
R3(config-subif)#exit

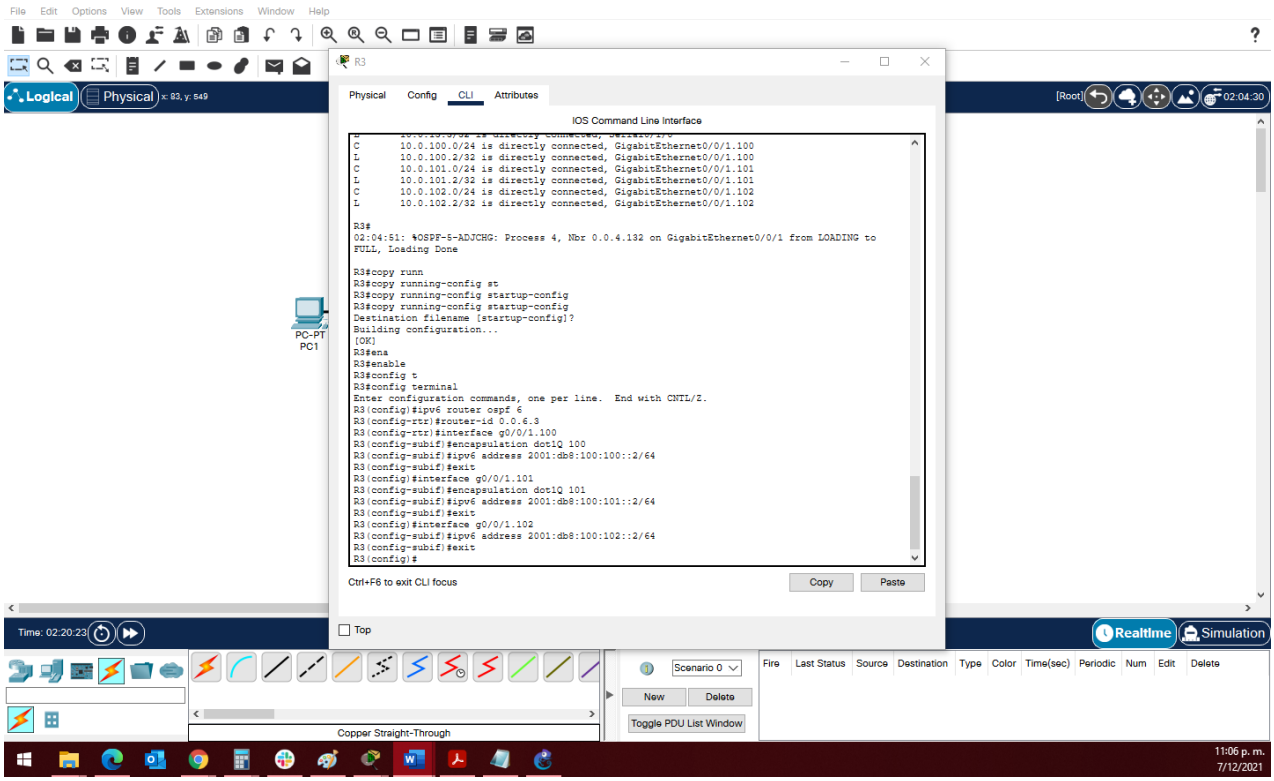


Figura 46 Anunciación de las VLAN en R3

Configuración de OSPFV3 y VLAN en R3 configuración OSPFv3 por puerto g0/0/1

```
R3(config)#Interface G0/0/1

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

Configuración OSPFv3 por puerto S0/1/0

```
R3(config)#Interface s0/1/0

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

configuración OSPFv3 por puerto g0/0/1.100 el cual es el ingreso de la VLAN 100

R3(config)#interface g0/0/1.100 R3(config-
subif)#ipv6 ospf 6 area 0R3(config-
subif)#exit

configuración OSPFv3 por puerto g0/0/1.101 el cual es el ingreso de la VLAN 101

R3(config)#interface g0/0/1.101 R3(config-
subif)#ipv6 ospf 6 area 0R3(config-
subif)#exit

configuración OSPFv3 por puerto g0/0/1.102 el cual es el ingreso de la VLAN 102

R3(config)#interface g0/0/1.102 R3(config-
subif)#ipv6 ospf 6 area 0R3(config-
subif)#exit

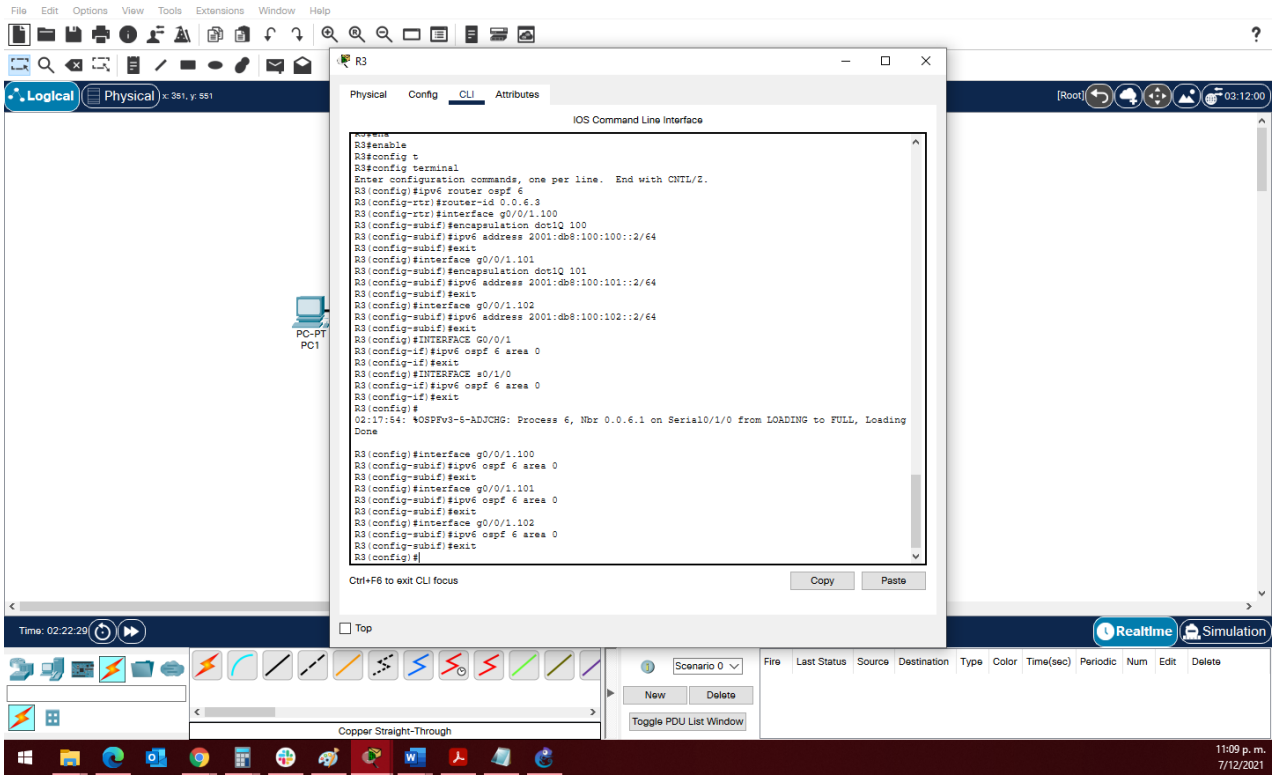


Figura 47 Configuración de OSPFV3 y VLAN en R3 Configuración OSPFv3 por puerto g0/0/1

Configuración de OSPFV3 en D1

Configuración D1 para protocolo OSPFV3 y configuración ID

D1(config)#ipv6 router ospf 6 D1(config-
rtr)#router-id 0.0.6.131D1(config-
rtr)#exit

Configuración OSPFv3 por puerto G1/0/11

```
D1(config)#interface g1/0/11
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

Configuración OSPFv3 por puerto VLAN100

```
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

Configuración OSPFv3 por puerto VLAN102

```
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

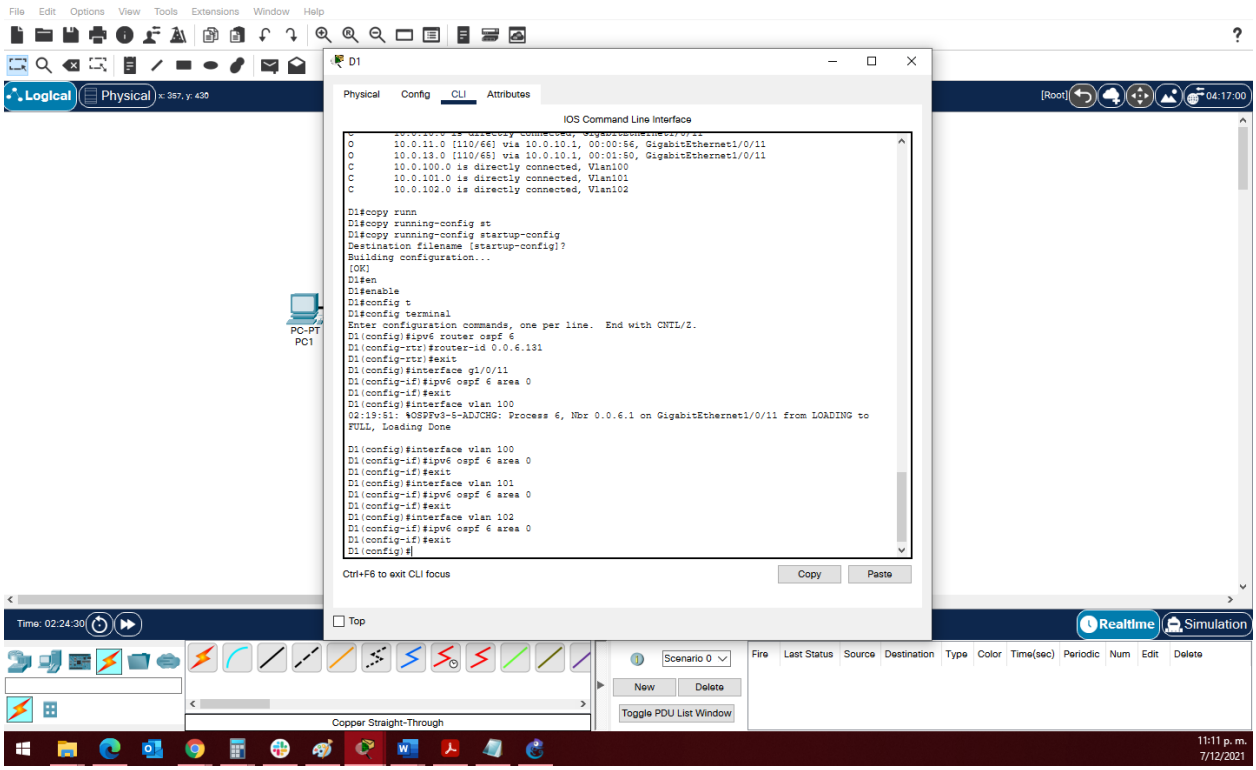


Figura 48 Configuración D1 para protocolo OSPFV3 y configuración ID

Configuración de OSPFV3 en D2

Configuración D2 para protocolo OSPFV3 y configuración ID

D2>Enable

D2#config terminal D2(config)#ipv6
router ospf 6 D2(config-rtr)#router-id
0.0.6.132D2(config-rtr)#exit

Configuración OSPFv3 por puerto G1/0/11

D2(config)#interface g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit

Configuración OSPFv3 por puerto VLAN100

D2(config)#interface vlan 100

D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit

Configuración OSPFv3 por puerto VLAN101

D2(config)#interface vlan 101

D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit

Configuración OSPFv3 por puerto VLAN102

D2(config)#interface vlan 102

D2(config-if)#ipv6 ospf 6 area

D2(config-if)#exit

Tabla de enrutamiento para R1, R2, D1 Y D2 con el protocolo OSPFV3

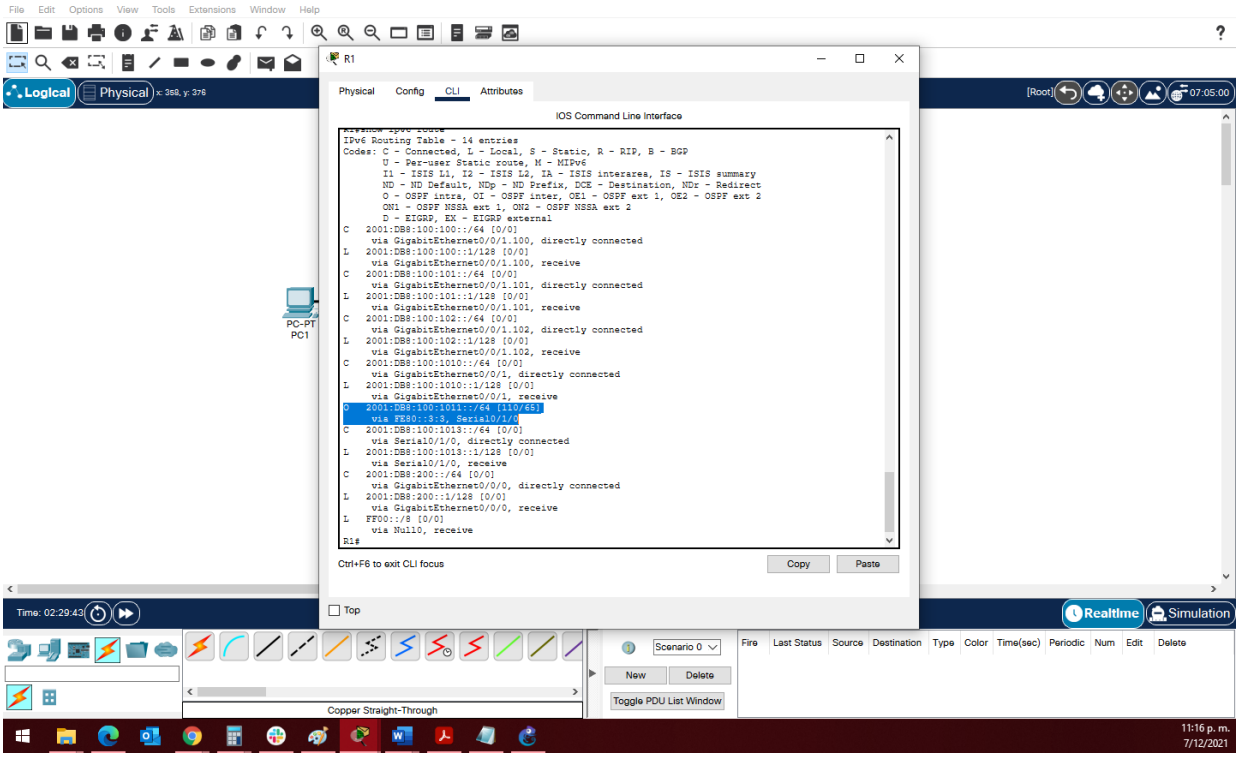


Figura 49 Enrutamiento OSPFv3 en R1

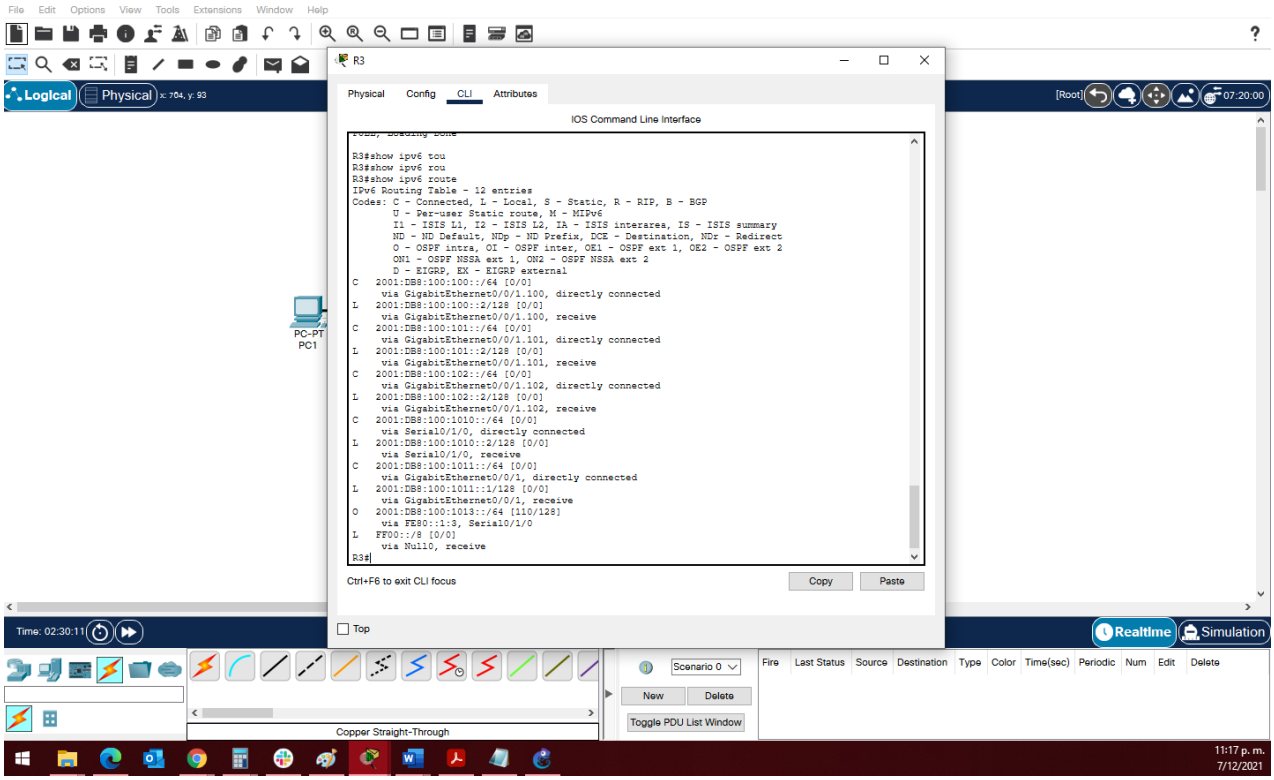


Figura 50 Enrutamiento OSPFv3 en R3

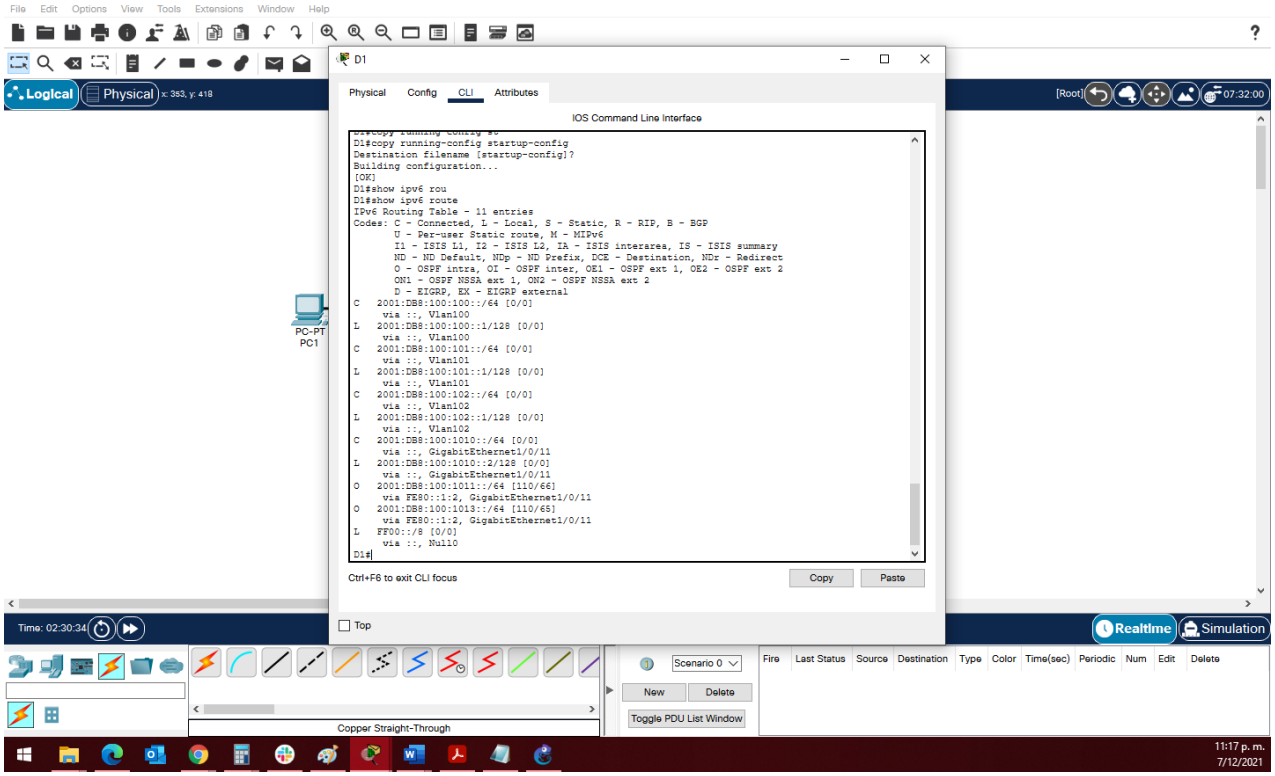


Figura 51 Enrutamiento OSPFv3 en D1

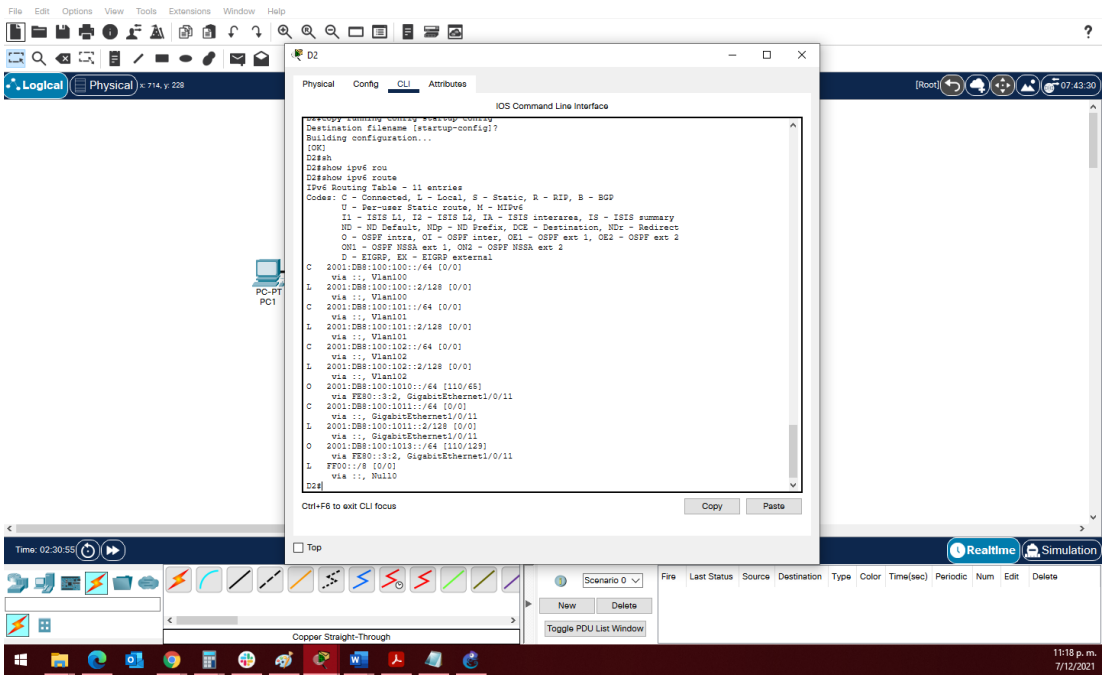


Figura 52 Enrutamiento OSPFv3 en D2

3.3 <u>En R2 en la “Red ISP”, configure MP-BGP.</u>

3.4 <u>En R1 en la “Red ISP”, configure MP-BGP.</u>

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. 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)

Figura 53 Configuración a realizar en parte 3 punto 3.3

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.

Figura 54 Configuración a realizar en parte 3 punto 3.4

Configuración R2 para protocolo de enrutamiento BGP

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

R2(config)#ip route 2.2.2.2 255.255.255.255 g0/0/1

R2(config)#ipv6 route 2001:db8:2222::1/128 g0/0/1

Configuración de protocolo BGP en R2

Router bgp 500

Bgp router-id 2.2.2.2

No bgp default ipv4-unicast

Neighbor 209.168.200.225 remote –as 300

Neighbor 2001:db8:200::1 remote-as 300

Address-family ipv4

Neitghbor 209.168.200.225 Active

Exit

Address-family ipv6

Neitghbor 2001:db8:200::1 Active

Configuración R1 para protocolo de enrutamiento BGP

Configure dos rutas resumen estáticas a la interfaz Null 0:

router bgp 300

network 10.0.0.0 mask 255.0.0.0

ip route 10.0.0.0 255.0.0.0 null0

network 2001:db8:100::/48

ip route 2001:db8:100::/48 null0

Configuración de protocolo BGP en R1

Router bgp 300

Bgp router-id 1.1.1.1

No bgp default ipv4-unicast

Neitghbor 209.168.200.226 remote –as 500Neitghbor 2001:db8:200::2 remote-as 500

Address-family ipv4

Neitghbor 209.168.200.226 ActiveExit

Address-family ipv6

Neitghbor 2001:db8:200::2 Active

Exit

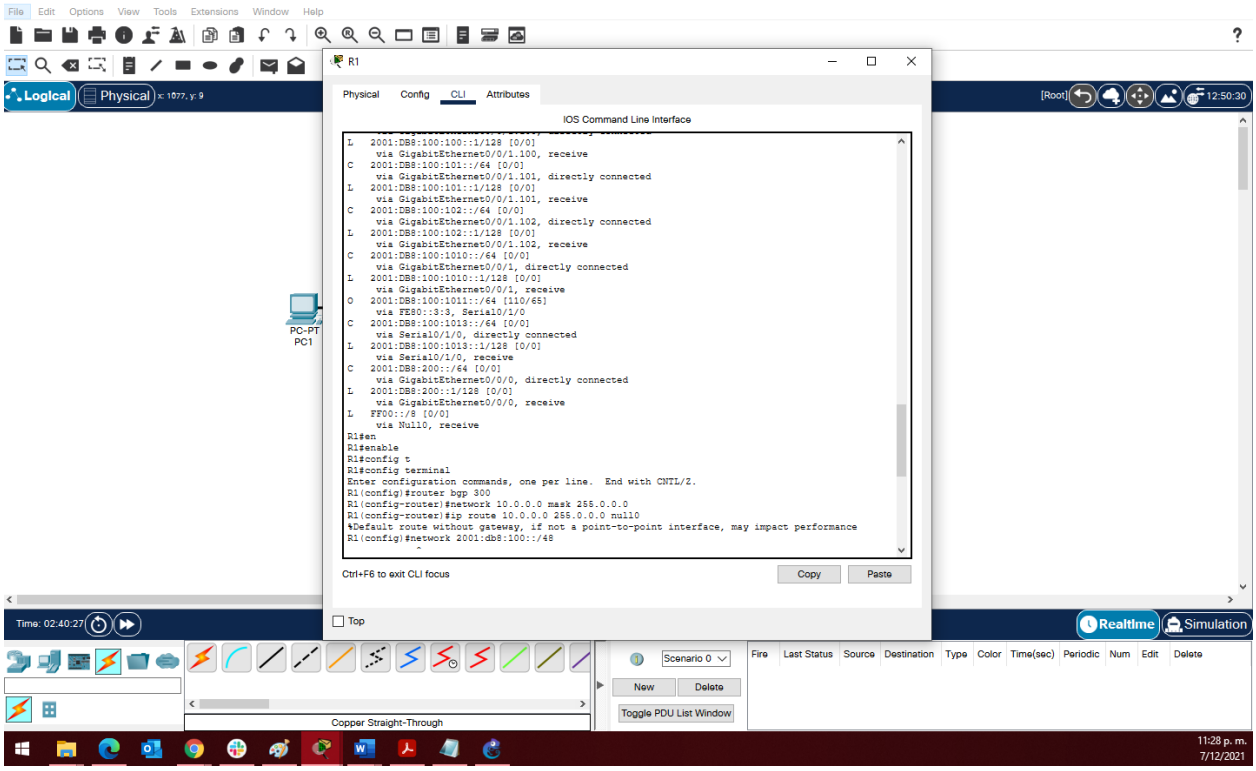


Figura 55 Configuración de protocolo BGP en R1

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

En esta parte vamos a configurar HSRP V2 para así promover la redundancia de primer salto para los terminales en la red

Adicional en esta parte se van a crear 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

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

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

Tarea#	Tarea	Especificación
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 R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 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.

Figura 56 Configuración a realizar en parte 4 puntos 4.1

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 R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 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.

Figura 57 Configuración a realizar en parte 4 puntos 4.2

CONFIGURACION IP SLA EN D1

Configuración IP SLA en D1 en ipv4

Ip sla 4

icmp-echo 10.0.10.1

Frequency 15

Exit

Ip sla Schedule 4 start-time now life forever

Configuración IP SLA en D1 en ipv6

Ip sla 6

icmp-echo 2001.db8.100:1010::1

Frequency 15

Exit

Ip sla Schedule 6 start-time now life forever

CONFIGURACION IP SLA EN D2

Configuración IP SLA en D1 en ipv4

Ip sla 4

icmp-echo 10.0.11.1 Frequency 15

Exit

Ip sla Schedule 4 start-time now life forever

Configuración IP SLA en D1 en ipv6

Ip sla 6

icmp-echo 2001.db8.100:1011::1

Frequency 15

Exit

Ip sla Schedule 6 start-time now life forever

4.3 En D1 configure HSRPv2

Habilitar HSRPV2 en Swicth D1 con IPV4

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.

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.

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.

Figura 58Configuración a realizar en parte 4 puntos 4.3

Explico la función de cada comando de HSRPV2 en VLAN100 de SWITCH D1 ya que para las otras VLANs se utilizan los mismos comandos teniendo en cuenta el cambio del grupo ip la ip virtual

Habilitar HSRPV2 en Swicth D1 con IPV4

VLAN 100

D1(config)#inter

D1 (config)#interface vlan 100

D1(config-if)#standby version 2

D1(config-if)#standby 104 ip 10.0.100.254

D1(config-if)#standby 104 priority 150

D1(config-if)#standby 104 preempt

D1(config-if)#no shutdown D1(config-if)#exit

VLAN 101

D1(config)#interface vlan 101

D1(config-if)#standby version 2

D1(config-if)#standby 114 ip 10.0.101.254

D1(config-if)#standby 114 preempt D1(config-if)#exit

D1(config)#

VLAN 102

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 124 preempt D1(config-if)#no shutdown D1(config-if)#exit

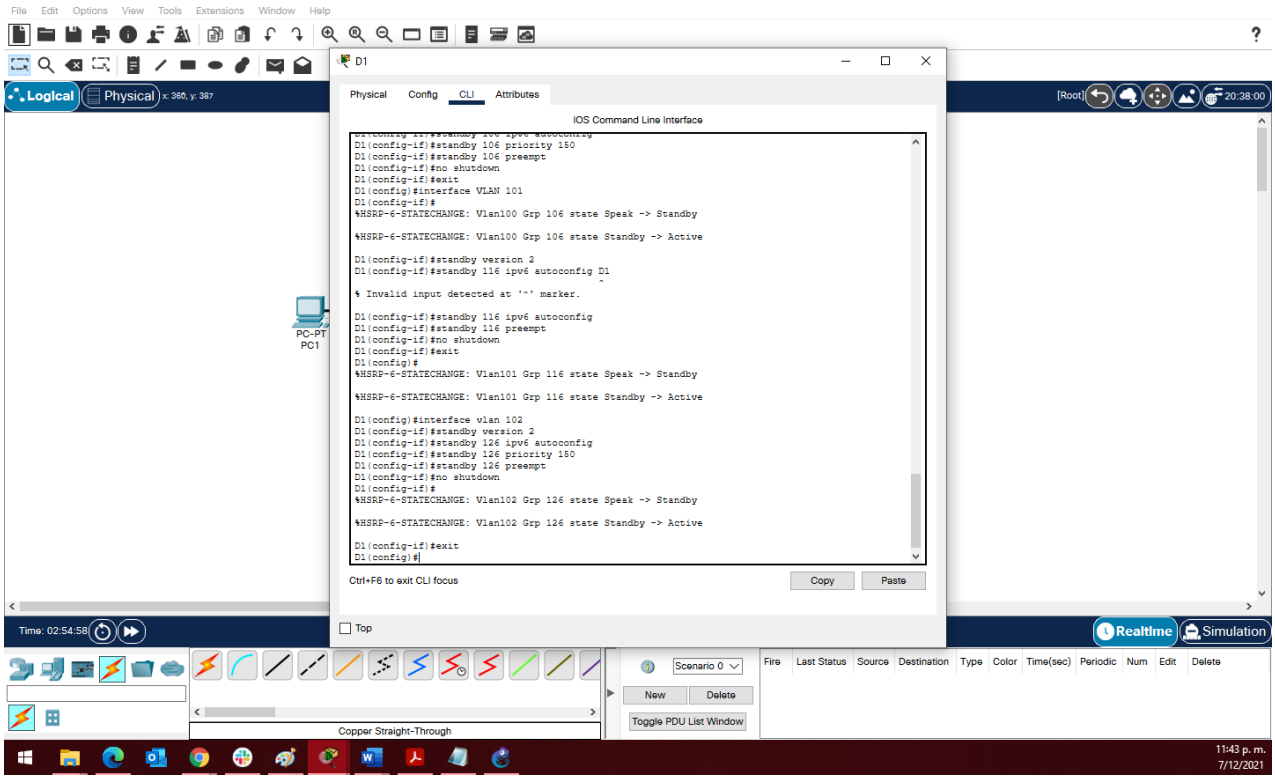


Figura 59 Habilitar HSRPV2 en Swicth D1 con IPV4

Habilitar HSRPV2 en Swicth D2 con IPV4

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

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

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

- Asigne la dirección IP virtual **10.0.101.254**.
- Establezca la prioridad del grupo en **150**.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

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

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

Figura 60 Puntos a desarrollar para habilitación HSRPV2 en D2

VLAN 100

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)#no shutdown D2(config-
if)#exit

VLAN 101

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)#exit

VLAN 102

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)#no shutdown D2(config-if)#exit

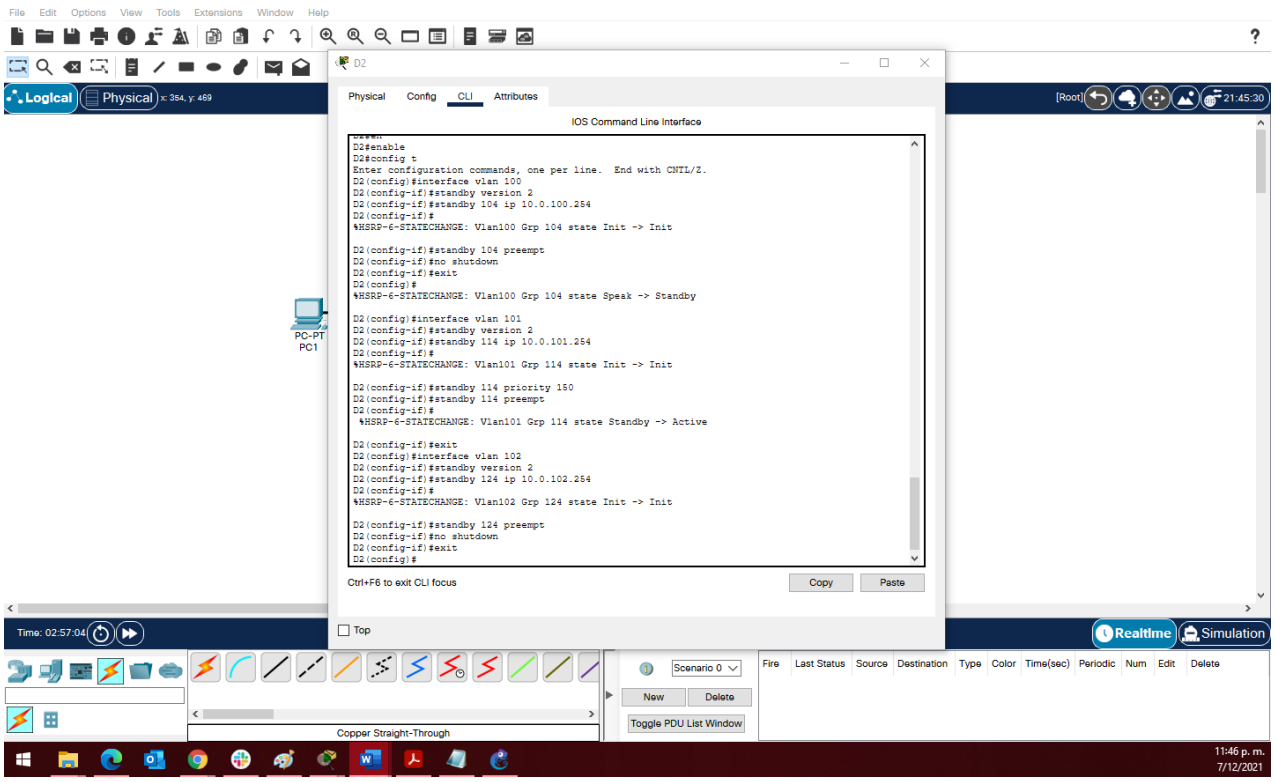


Figura 61 Habilitar HSRPV2 en Swicth D1 con IPV6

Habilitar HSRPV2 en Swicth D2 con IPV6

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.

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.

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.

Figura 62 Puntos a desarrollar para habilitación HSRPV2 en D1 CON i

VLAN 101

D2(config)#interface VLAN 101

D2(config-if)#standby version 2

D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150

D2(config-if)#standby 116 preempt
D2(config-if)#no shutdown D2(config-
if)#exit

VLAN 102

D2(config)#interface vlan 102

D2(config-if)#standby version 2

D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt D2(config-
if)#no shutdown

D2(config-if)#exit

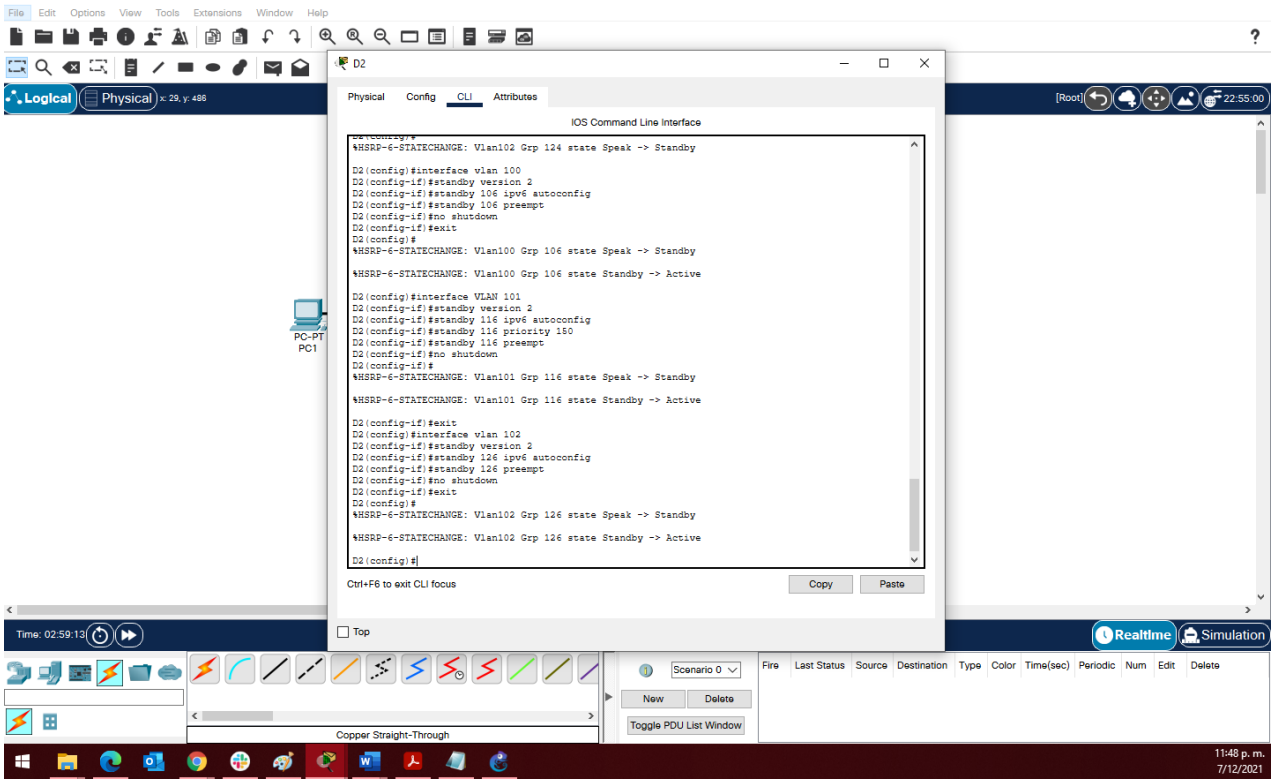


Figura 63 Configuración n de protocolo HSRPV2 en D1

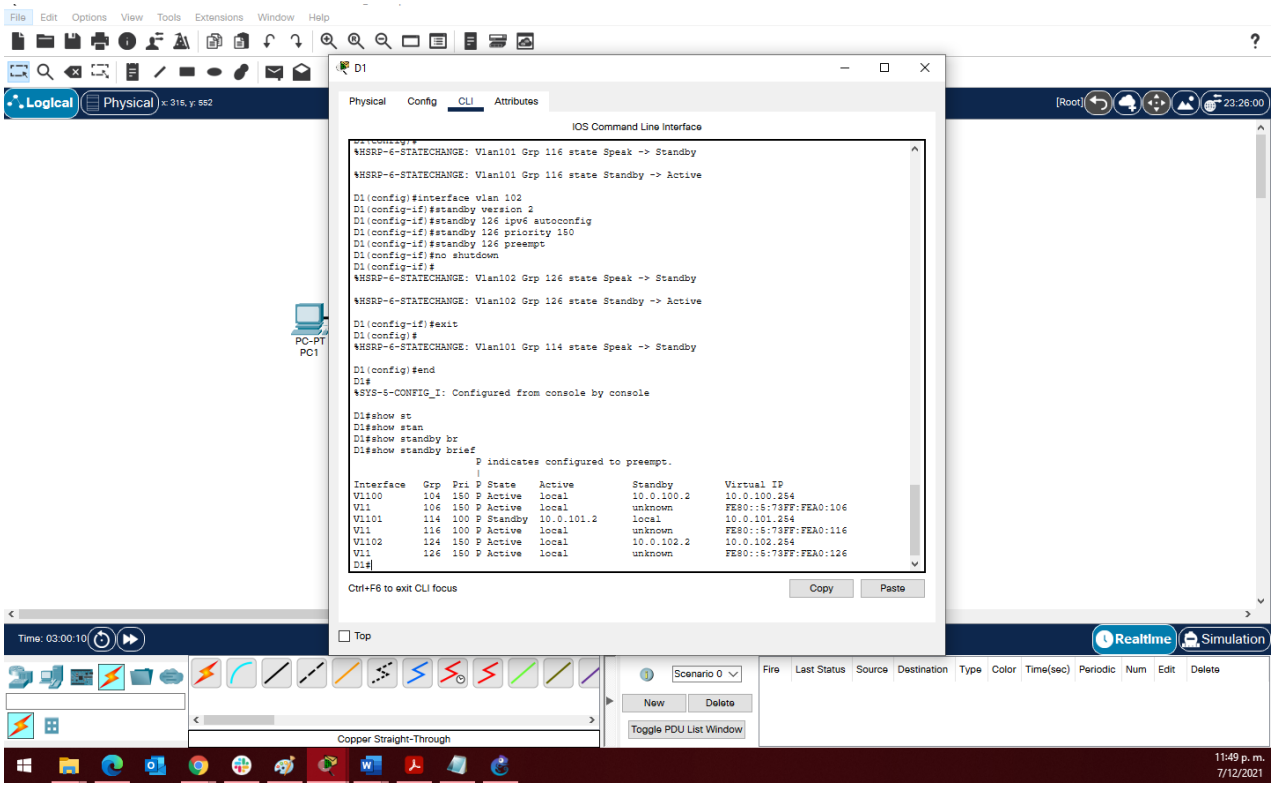


Figura 64 Verificación de protocolo HSRPV2 configurado en D1

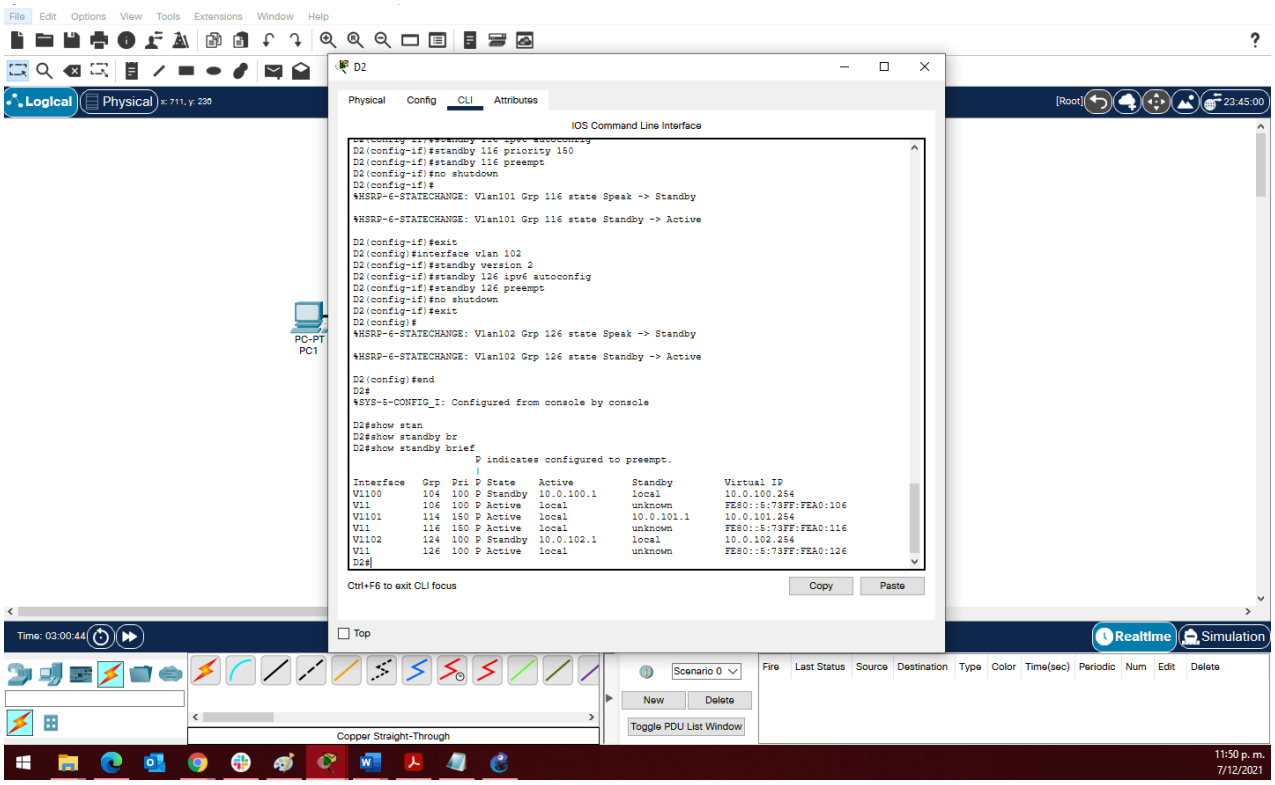


Figura 65 Verificación de protocolo HSRPV2 configurado en D2

Parte 5: Seguridad

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

Se debe habilitar 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.

Se creará 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

En todos los dispositivos (excepto R2), Se habilitará AAA.

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

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

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

5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.

Figura 66 Puntos a desarrollar en Parte 5

EN SWITCH D1

D1(config)#enable secret cisco12345cisco

D1(config)#end D1#disable

D1>Enable

Password:

D1#config terminal

D1(config)#enable secret 15

D1(config)#enable secret 15 cisco12345cisco

D1(config)#username sadmin privilege 15 secret cisco12345cisco

D1(config)#do wri

D1(config)#

D1(config)#aaa new-model

D1(config)#aaa authentication login default local-case

VERIFICACIONES DE COMANDOS INGRESADOS EN D1

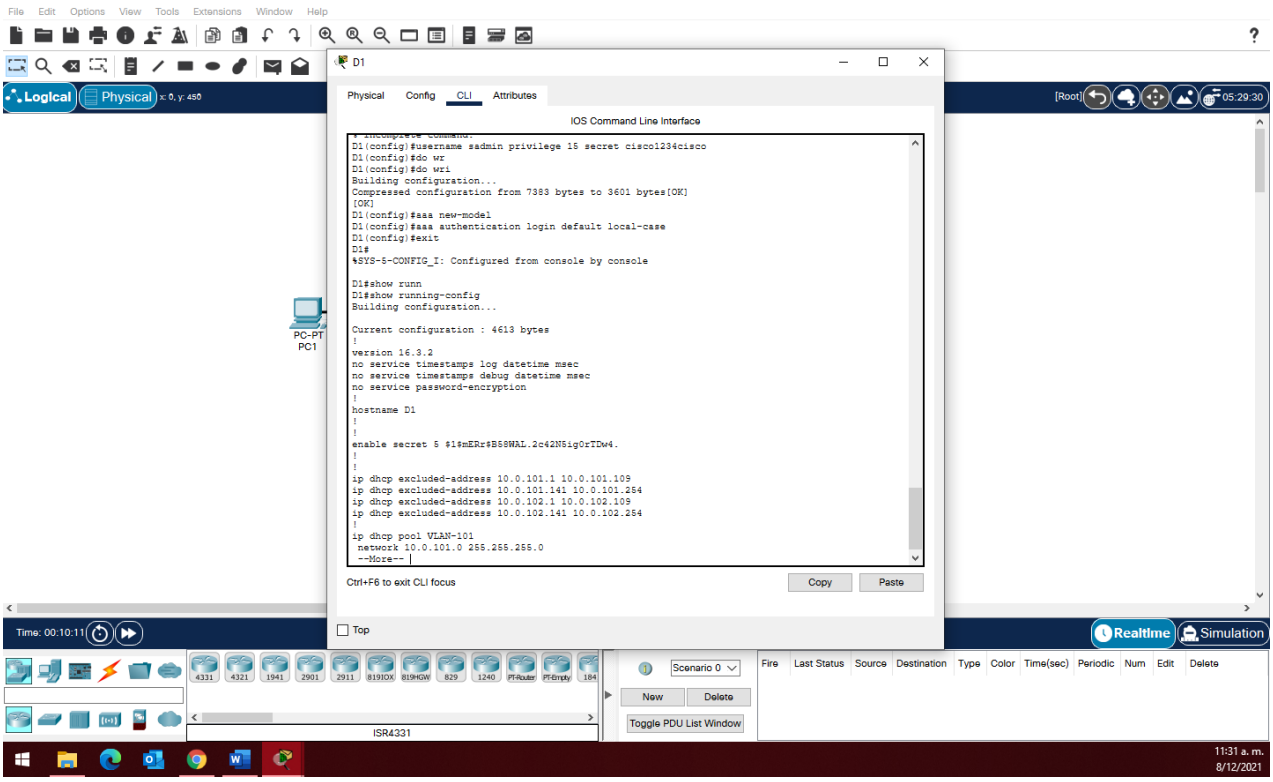


Figura 67 verificación de contraseña enable secret configurada y encriptada

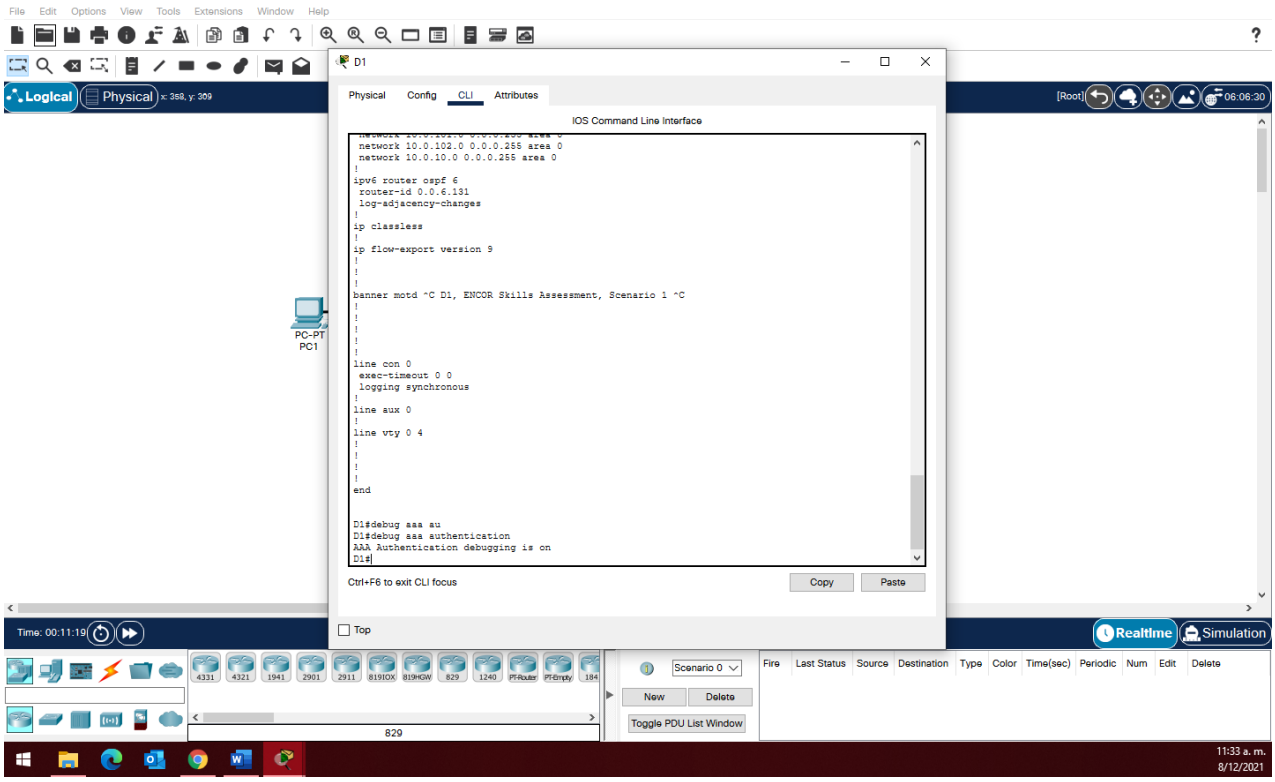


Figura 68 verificación AAA ya configurado

EN SWITCH D2

D2>Enable

D2#config terminal

D2(config)#enable secret cisco12345cisco

D2(config)#end
D2#disable

D2>Enable

Password:

D2#config terminal D1(config)#enable secret 15

D2(config)#enable secret 15 cisco12345cisco

D2(config)#username sadmin privilege 15 secret cisco12345cisco

D2(config)#do wri

D2(config)#

D2(config)#aaa new-model

D2(config)#aaa authentication login default local-case

VERIFICACIONES DE COMANDOS INGRESADOS EN D2

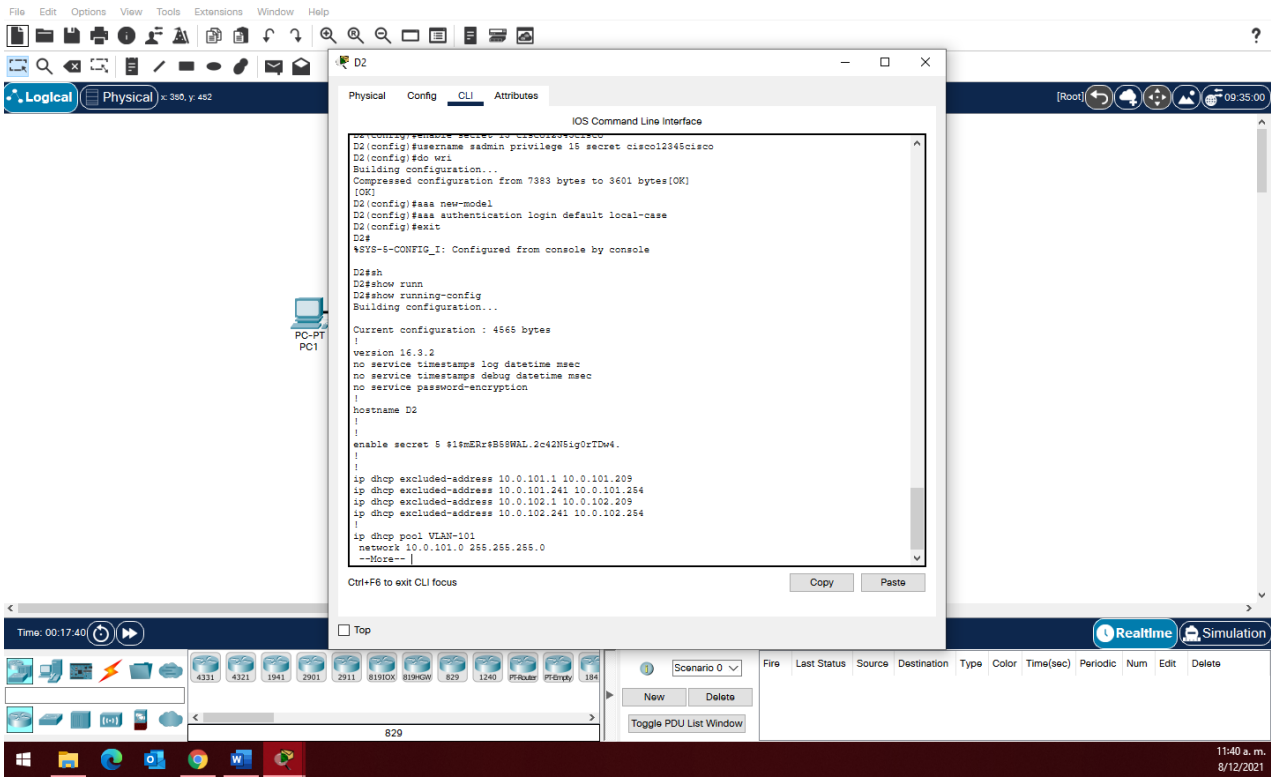


Figura 69 verificación de contraseña enable secret configurada y encriptada

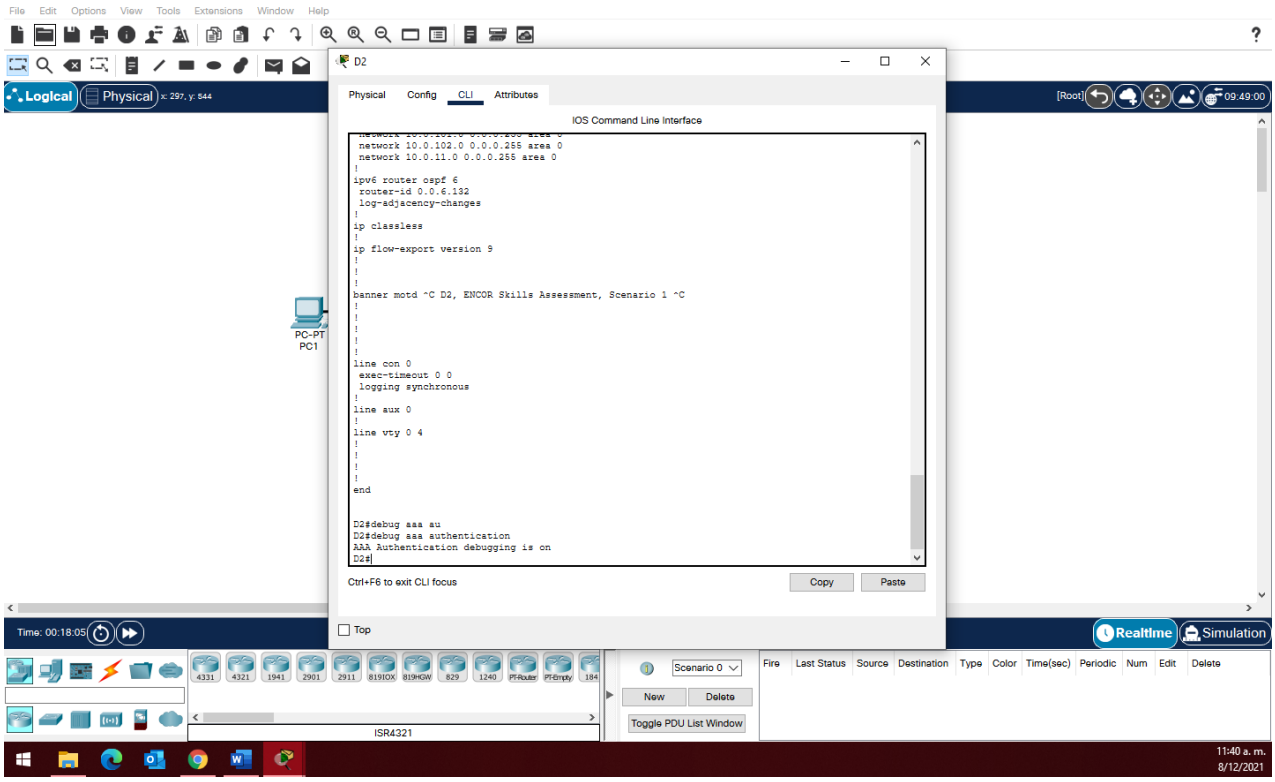


Figura 70 Verificación AAA ya configurado

EN SWITCH A1

A1>Enable

A1#config terminal

A1(config)#enable secret cisco12345cisco

A1(config)#end
A1#disable

A1>ENABLE

Password:

A1#config terminal

D1(config)#enable secret 15

A1(config)#enable secret 15 cisco12345cisco

A1(config)#username sadmin privilege 15 secret cisco12345cisco

A1(config)#do wri

A1(config)#

A1(config)#aaa new-model

A1(config)#aaa authentication login default local-case

VERIFICACIONES DE COMANDOS INGRESADOS EN A1

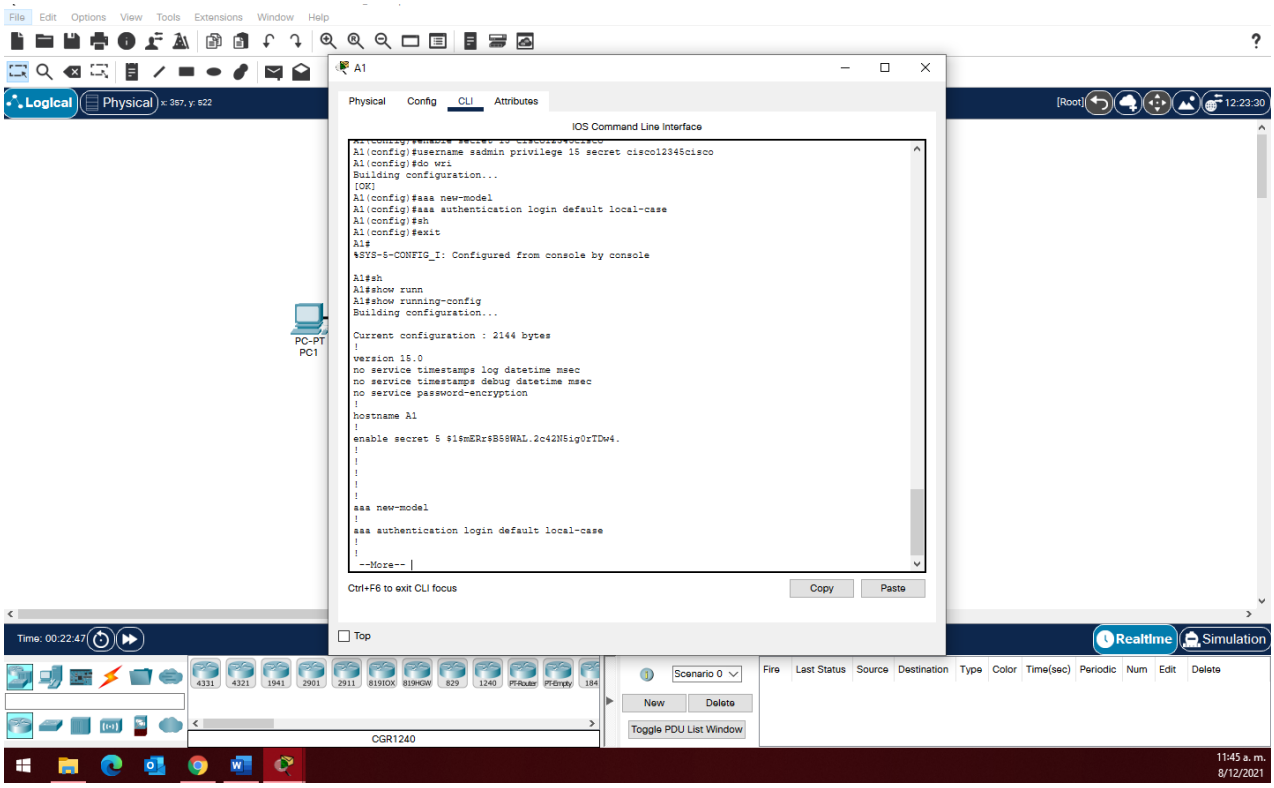


Figura 71 verificación de contraseña enable secret configurada y encriptada

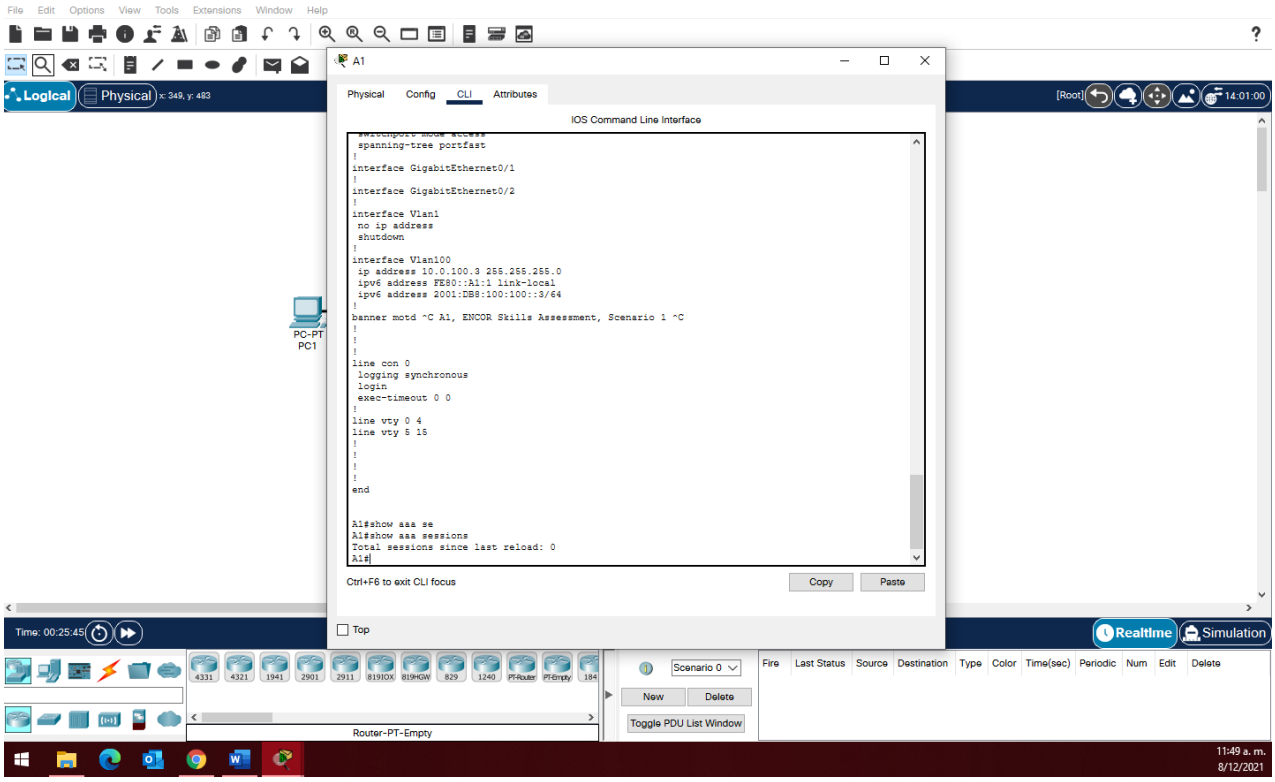


Figura 72 Verificación AAA ya configurado

EN ROUTER R1

R1>Enable

R1#config terminal

R1(config)#enable secret cisco12345cisco

R1(config)#end
R1#disable

R1>Enable

Password:

R1#config terminal

D1(config)#enable secret 15

R1(config)#enable secret 15 cisco12345cisco

R1(config)#username sadmin privilege 15 secret cisco12345cisco

R1(config)#do wri

R1(config)#

R1(config)#aaa new-model

R1(config)#aaa authentication login default local-case

VERIFICACIONES DE COMANDOS INGRESADOS EN R1

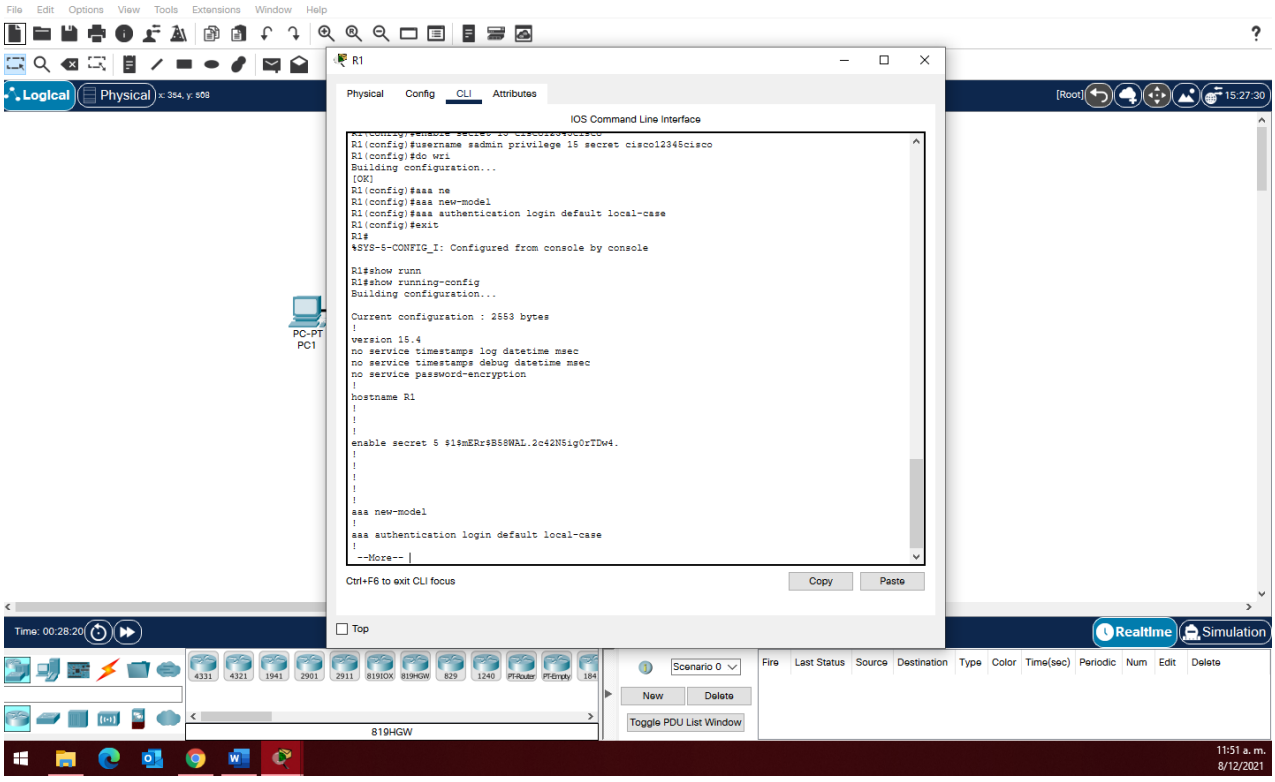


Figura 73 verificación de contraseña enable secret configurada y encriptada

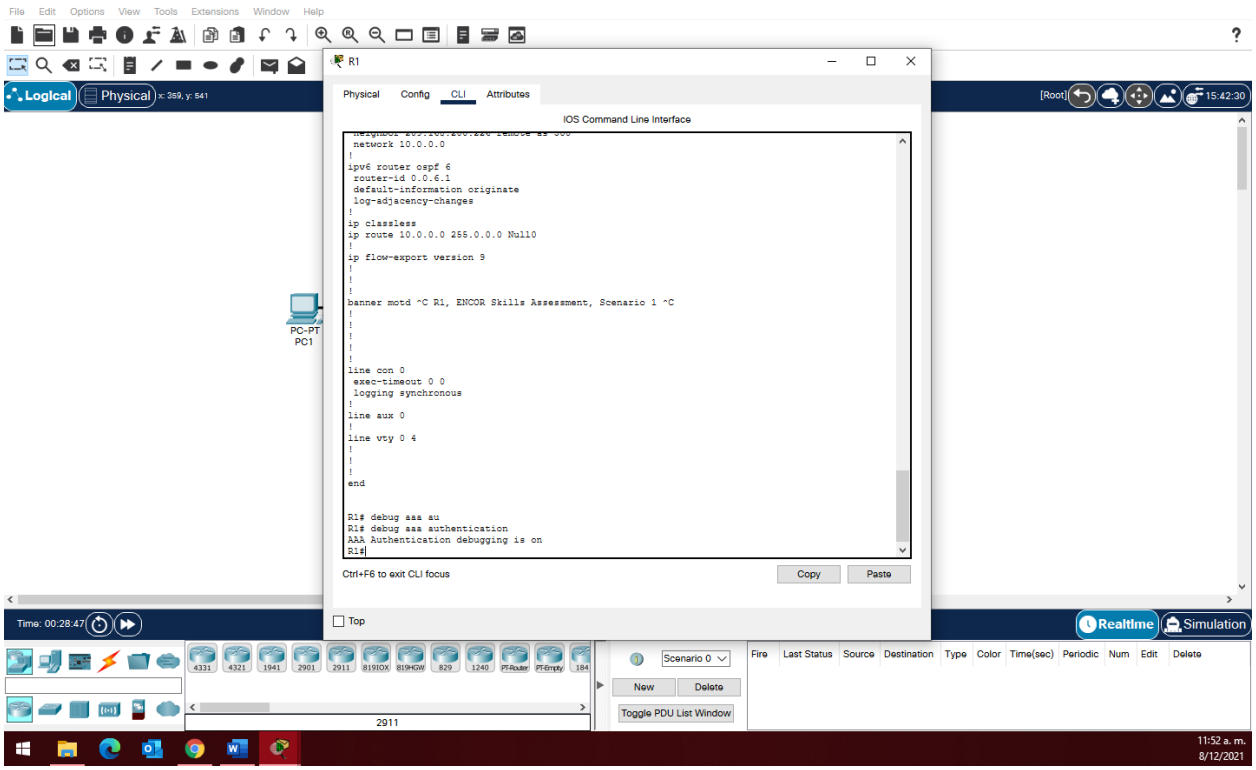


Figura 74 verificación AAA ya configurado

EN ROUTER R3

R3>Enable

R3#config terminal

R3(config)#enable secret cisco12345cisco

R3(config)#end
R3#disable

R3>Enable

Password:

R3#config terminal

D1(config)#enable secret 15

R3(config)#enable secret 15 cisco12345cisco

R3(config)#username sadmin privilege 15 secret cisco12345cisco

R3(config)#do wri

R3(config)#

R3(config)#aaa new-model

R3(config)#aaa authentication login default local-case

VERIFICACIONES DE COMANDOS INGRESADOS EN R3

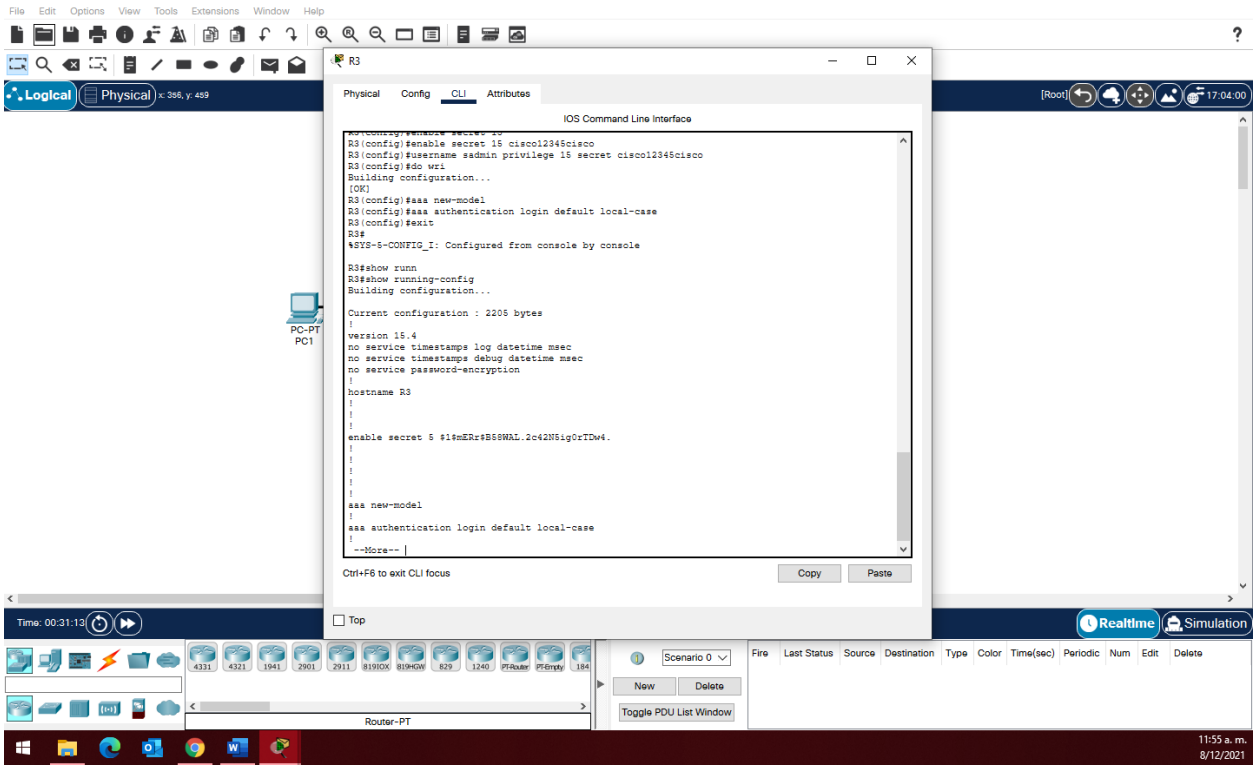


Figura 75 verificación de contraseña enable secret configurada y encriptada

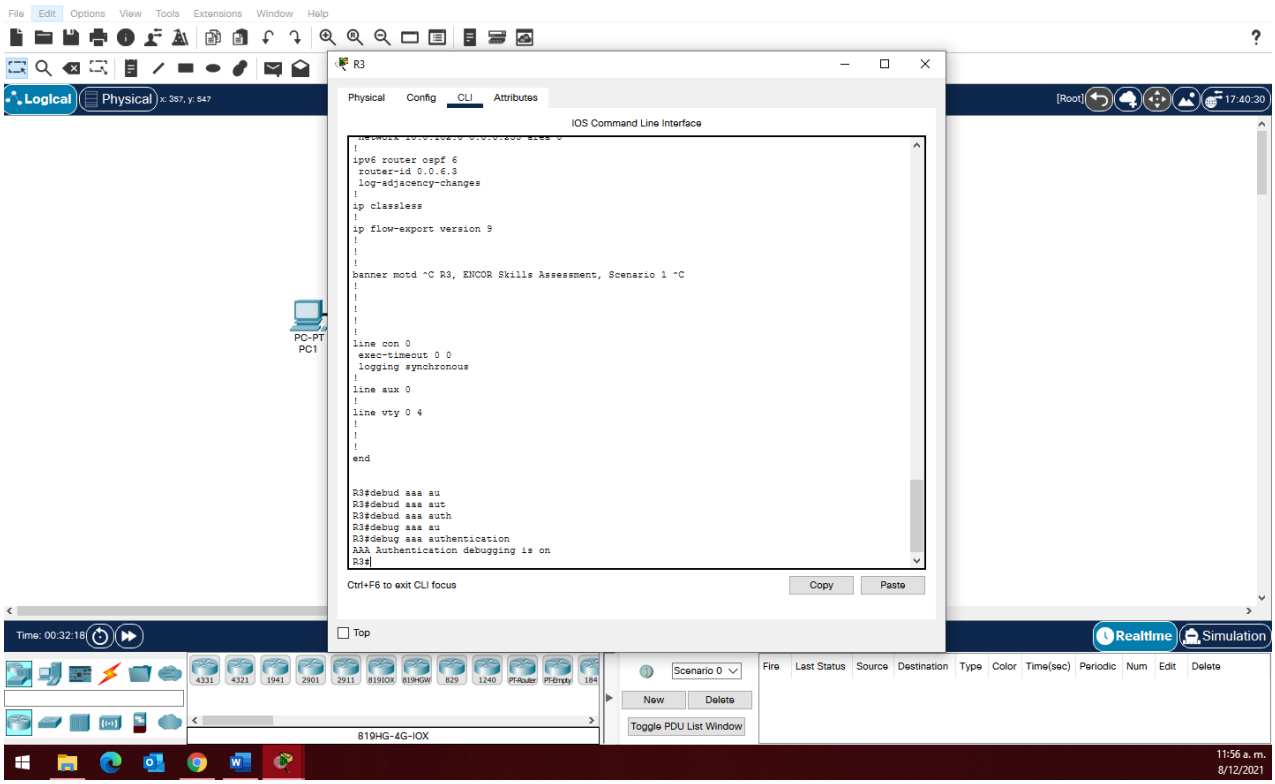


Figura 76 verificación AAA ya configurado

EN ROUTER R2

R2>Enable

R2#config terminal

R2(config)#enable secret cisco12345cisco

R2(config)#end

R2#disable

R2>Enable

Password:

R2#config terminal

D1(config)#enable secret 15

R2(config)#enable secret 15 cisco12345cisco

R2(config)#username sadmin privilege 15 secret cisco12345cisco

R2(config)#do wri

R2(config)#

VERIFICACIONES DE COMANDOS INGRESADOS EN R3

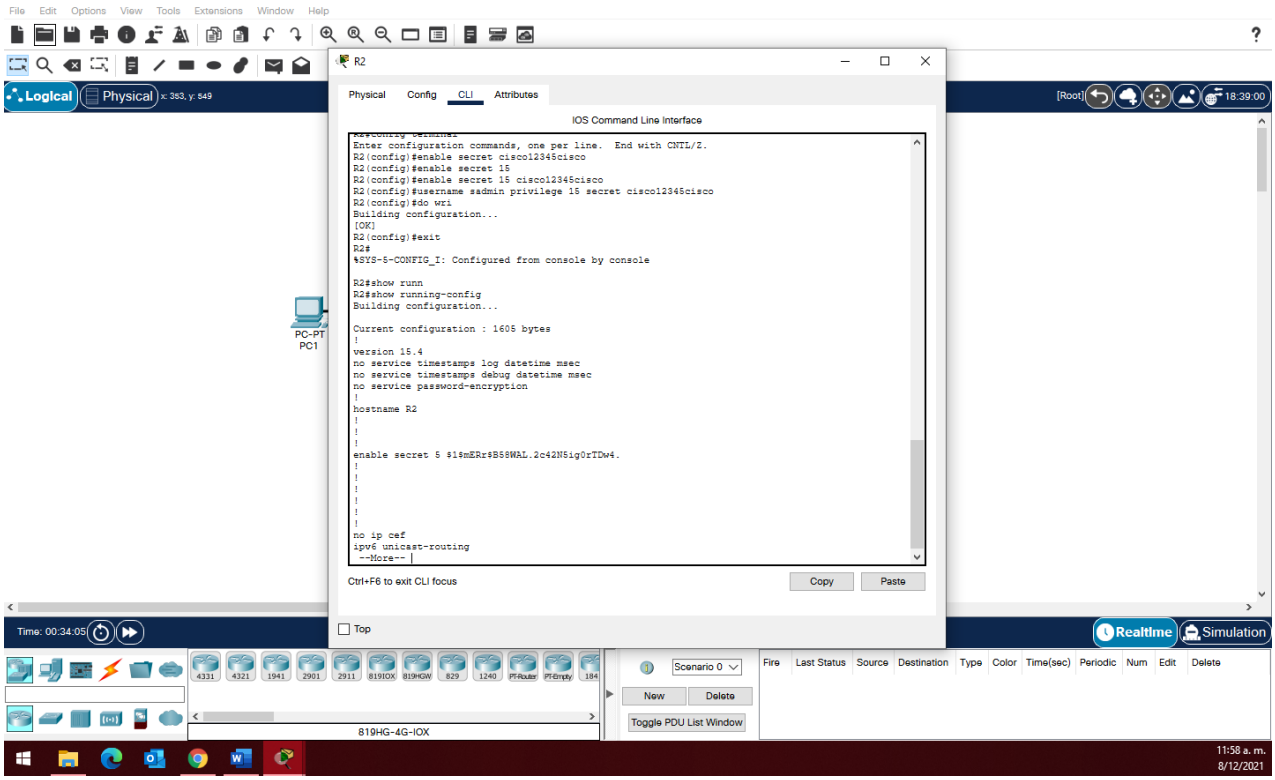


Figura 77 verificación de contraseña enable secret configurada y encriptada

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

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

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

Se configurará 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 (ccnalearner.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: $trongPass

Se proporcionara 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.)

Para verificar se cerraran e iniciaremos 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

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

Figura 78 configuración a realizar paso 5

CONFIGURACIÓN DE SERVIDOR RADIUS

Explico los comandos que se utilizaron en R1 ya que en los otros dispositivos utilice los mismos comandos para la activación de protocolo AAA y configuración de servidor RADIUS.

Configuración de servidor RADIUS EN R1

```
R1#config terminal
R1(config)#aaa new-model
R1(config)#radius-server hos 10.0.100.254 key $trongPass
R1(config)#aaa authentication login default group radius local
R1(config)#
R1(config)#line vty 0 15
R1(config-line)#login aut
```

R1(config-line)#login authentication default
R1(config-line)#exit

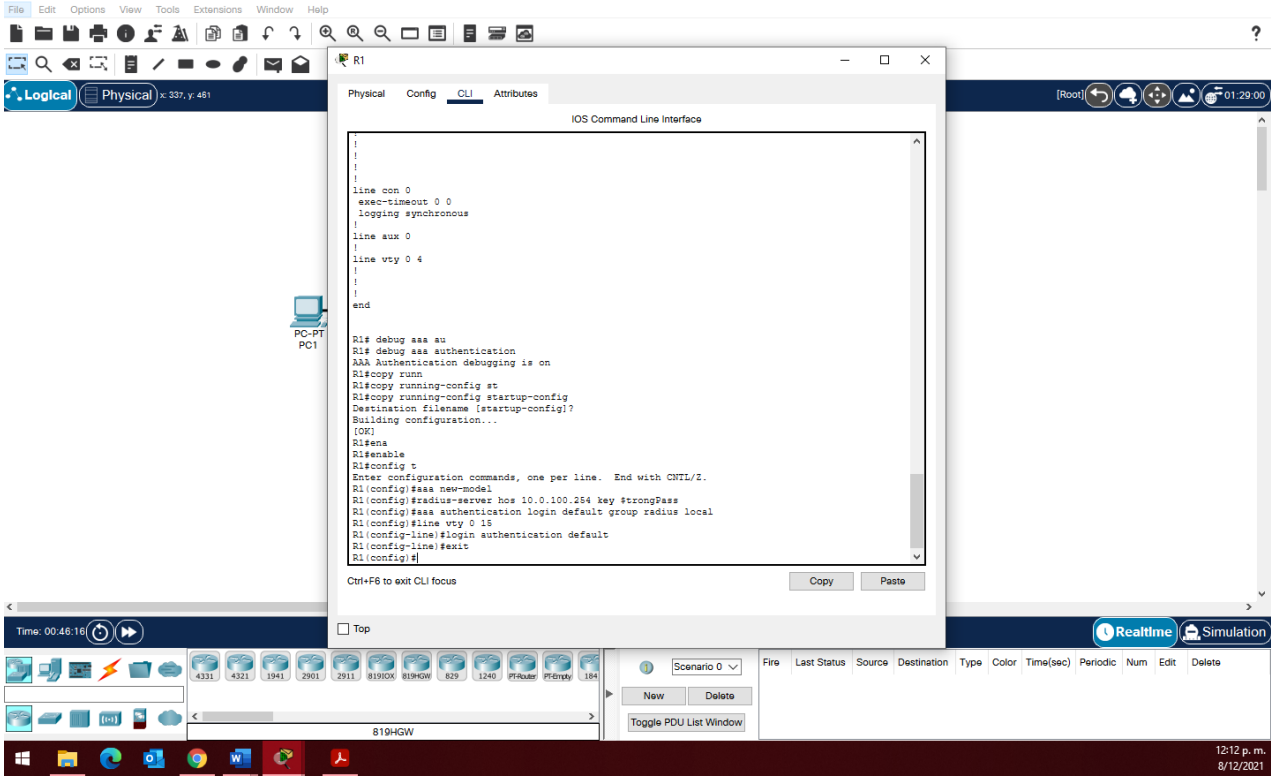


Figura 79 configuración de servidor radius en r1

CONFIGURACIÓN DE SERVIDOR RADIUS EN R3

R3#config terminal R3(config)#aaa
new-model

R3(config)#radius-server hos 10.0.100.254 key $trongPass
R3(config)#aaa authentication login default group radius local
R3(config)#

R3(config)#line vty 0 15
R3(config-line)#login aut

R3(config-line)#login authentication default
R3(config-line)#exit

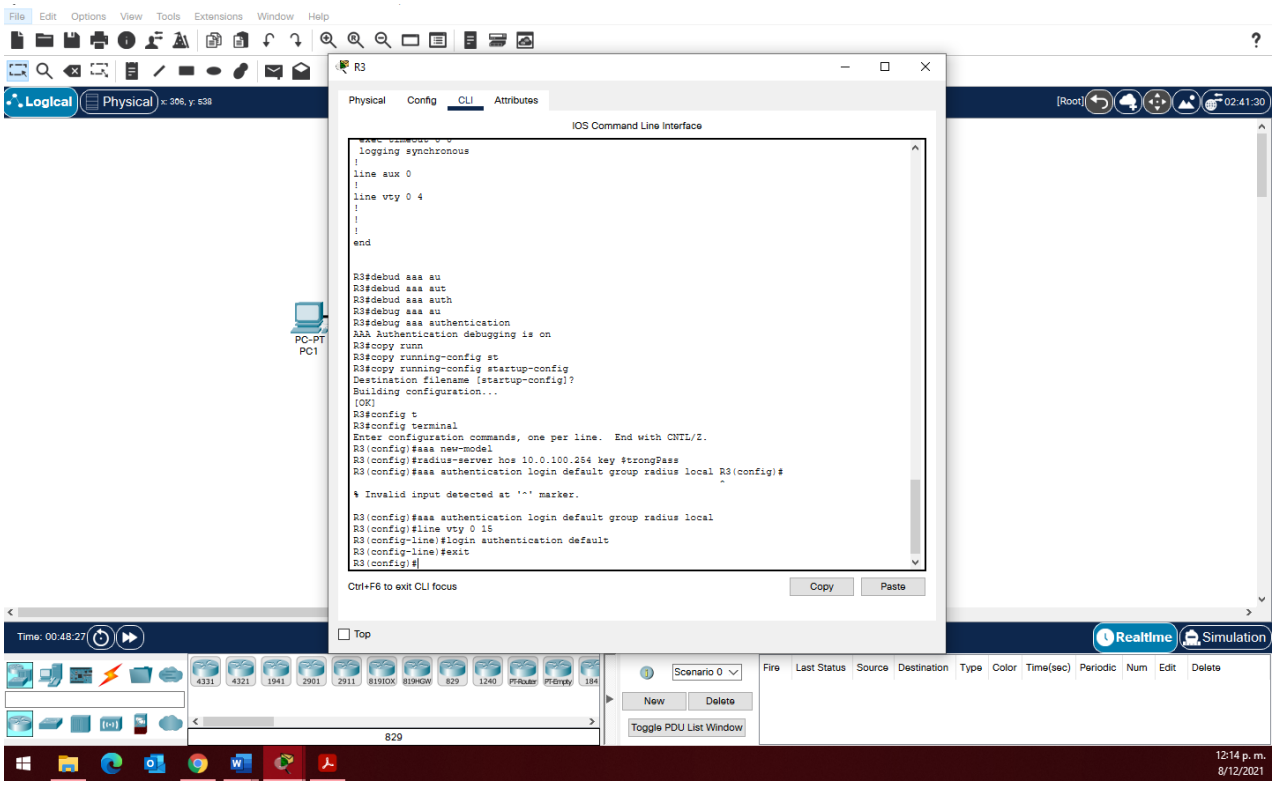


Figura 80 configuración de servidor radius en r3

CONFIGURACIÓN DE SERVIDOR RADIUS EN D1

D1#config terminal. D1(config)#aaa new-model

D1(config)#radius-server host 10.0.100.254 key $trongPass

D1(config)#aaa authentication login default group radius local

D1(config)#

D1(config)#line vty 0 15

D1(configline)#login aut

D1(config-line)#login authentication default

D1(config-line)#exit

CONFIGURACION DE SERVIDOR RADIUS EN D2

D2#config terminal D2(config)#aaa new-model

D2(config)#radius-server hos 10.0.100.254 key $trongPass

D2(config)#aaa authentication login default group radius local

D2(config)#

D2(config)#line vty 0 15

D2(config-line)#login aut

D2(config-line)#login authentication default

D2(config-line)#exit

CONFIGURACION DE SERVIDOR RADIUS EN A1

A1#config terminal A1(config)#aaa new-model

A1(config)#radius-server hos 10.0.100.254 key $trongPass

A1(config)#aaa authentication login default group radius local

A1(config)#

A1(config)#line vty 0 15

A1(config-line)#login aut

A1(config-line)#login authentication default

R3(config-line)#exit

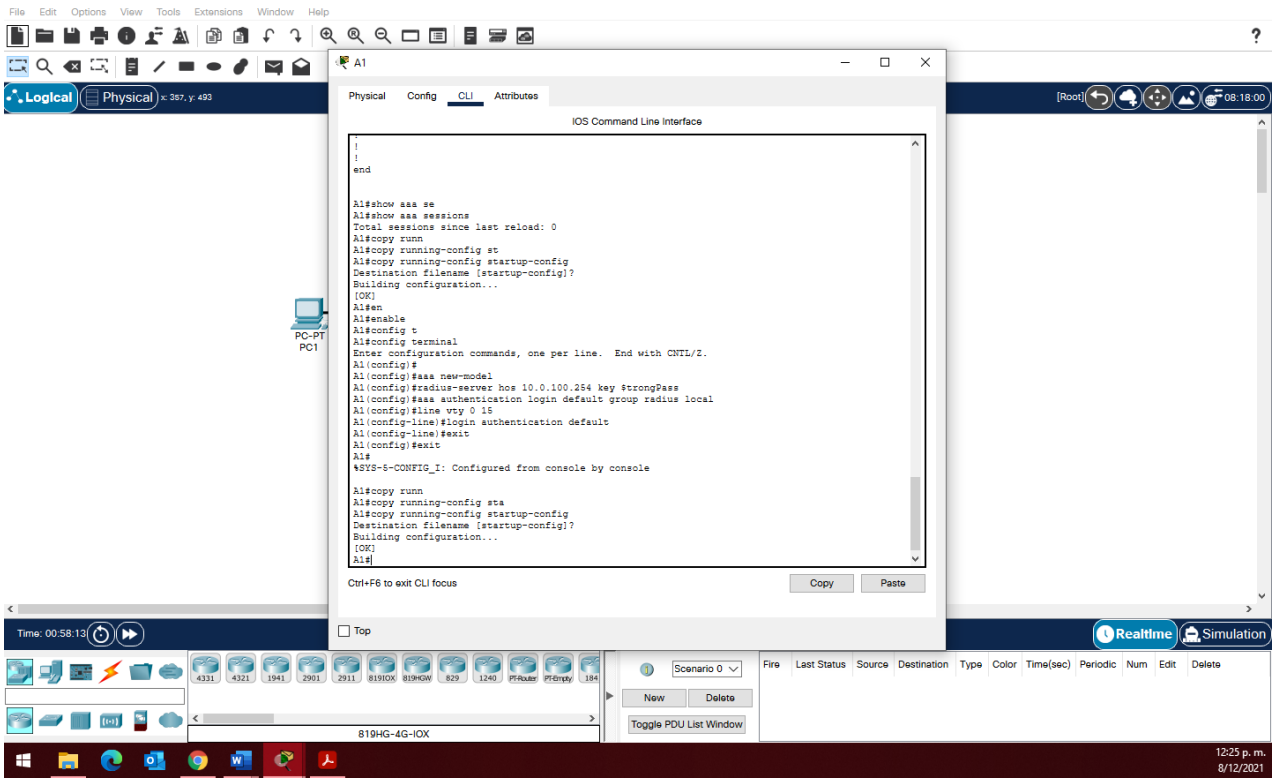


Figura 81 configuración de servidor radius en A1

Parte 6: Configure las funciones de Administración de Red

Nota: A partir de este momento voy a dejar los comandos a utilizar para las configuraciones ya que por las limitaciones que tiene Packet Tracer no me deja ingresarlos al software al igual que algunos comandos que especifique en puntos anteriores.

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.

Figura 82 Puntos a realizar en Parte 6 Puntos 6.1 y 6.2

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 12:29:20 08 December 2021

R2# Clock set 12:29:20 08 December 2021

R3# Clock set 12:29:20 08 December 2021

D1# Clock set 12:29:20 08 December 2021

D2# Clock set 12:29:20 08 December 2021

A1# Clock set 12:29:20 08 December 2021

6.2 Configure R2 como un NTP maestro.

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

R2(config)# ntp master 3

Configuración de protocolo NTP

Especificaciones:

Configurar R2 como NTP maestro en el nivel de estrato 3.

Se procede a realizar configuración del servicio NTP para que los dispositivos mantengan una sincronización de reloj, se configura R2 como maestro.

Comandos utilizados en R2:

enable

config t

ntp master 3

exit

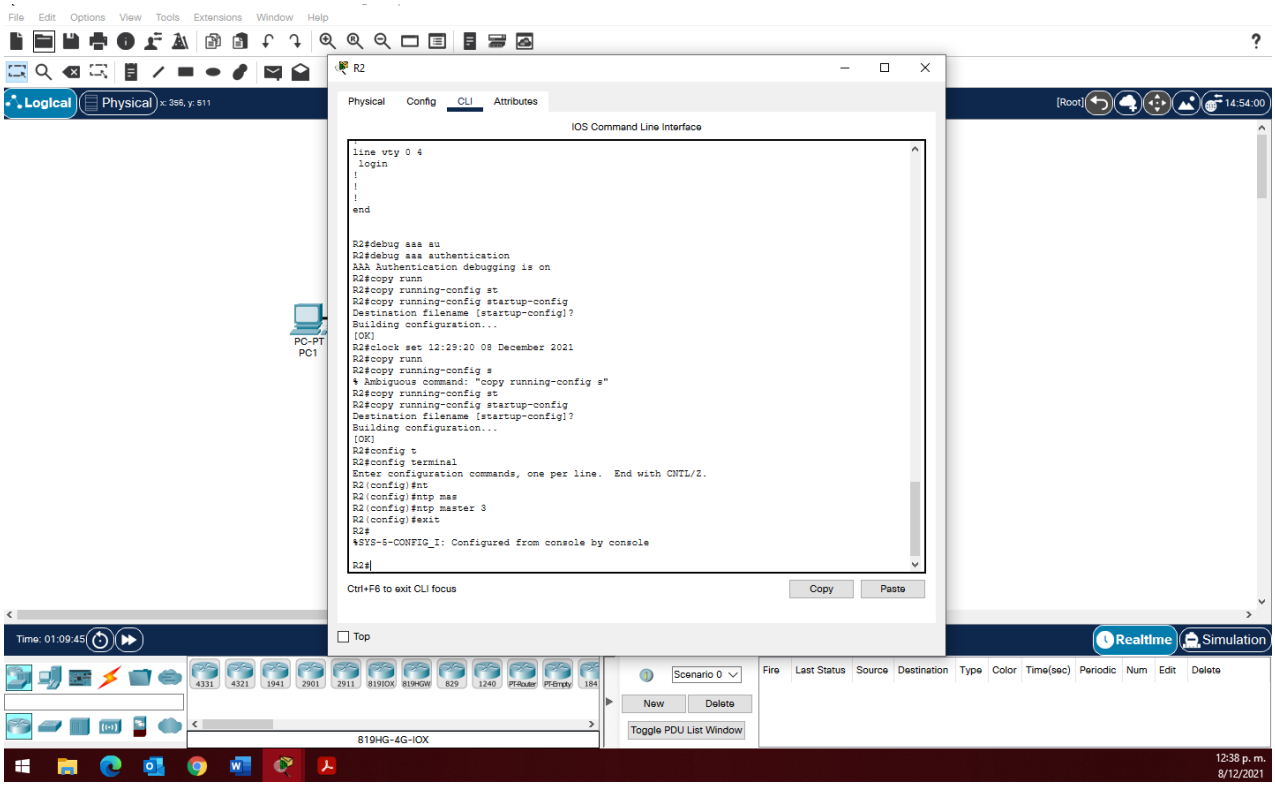


Figura 83 Configuración NTP R2

Validación configuración en R2

Comando utilizado: show run | include ntp

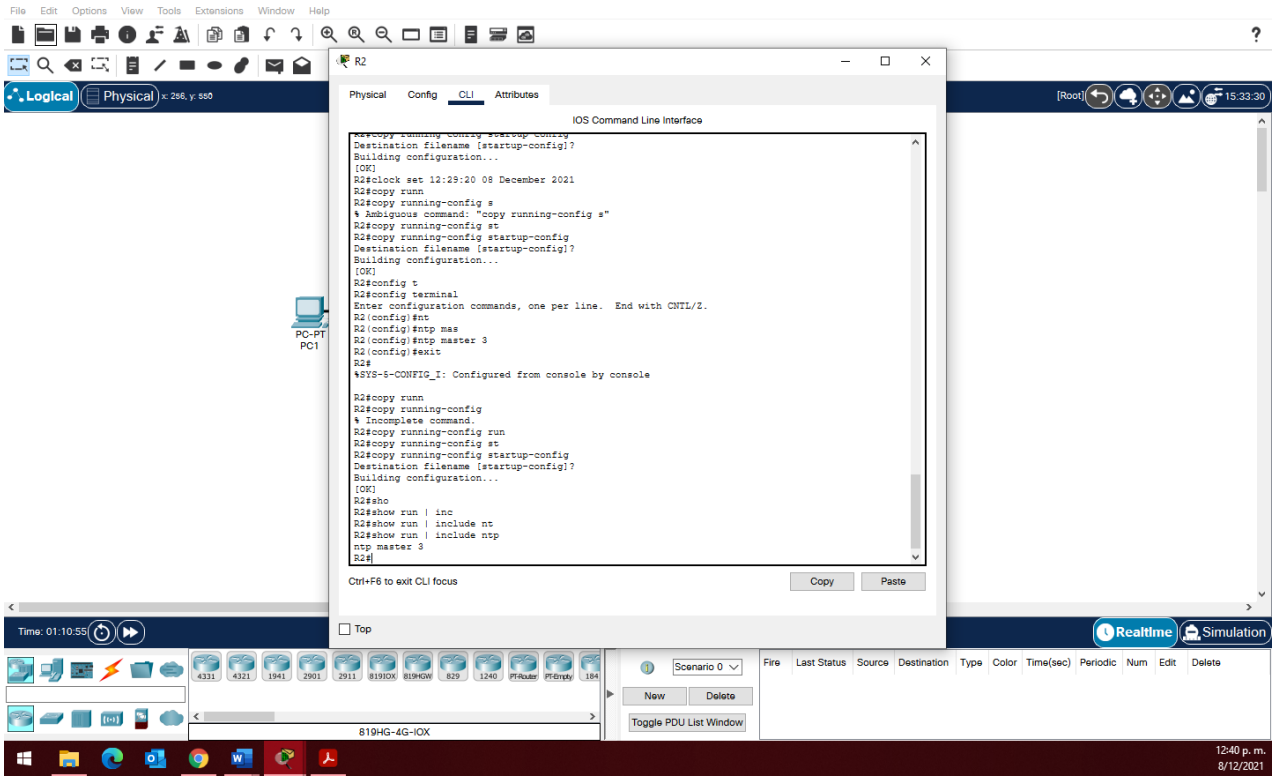


Figura 84 Validación NTP R2

Tarea#	Tarea	Especificación
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.
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.

Figura 85 Puntos a realizar en Parte 6 Puntos 6.3 y 6.4

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

Especificaciones:

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.

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

Especificaciones:

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

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.

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 su nombre.

• Establezca el community string en ENCORSA.

- En R3, D1, y D2, habilite el envío de traps config y ospf.
- En R1, habilite el envío de traps bgp, config, y ospf.
- En A1, habilite el envío de traps config.

Configuración de sincronización de reloj en los dispositivos, R1 sincronizara hacia R2 que se encuentra como maestro, y habilitación de protocolo SNMP para intercambio de administración entre los dispositivos de la Topología y los correspondientes mensajes de trap que permita sondear la información que se transmite en la red

Configuraciones en R1

Comandos utilizados:

Enable

configt

ntp server 2.2.2.2 logging trap
warning logging host
10.0.100.5logging on

ip access-list standard SNMP-NMS

permit host 10.0.100.5

exit

VALIDACION SINCRONIZACIÓN NTP EN R1 HACIA R2

Comando utilizado: show ntp status | include stratum

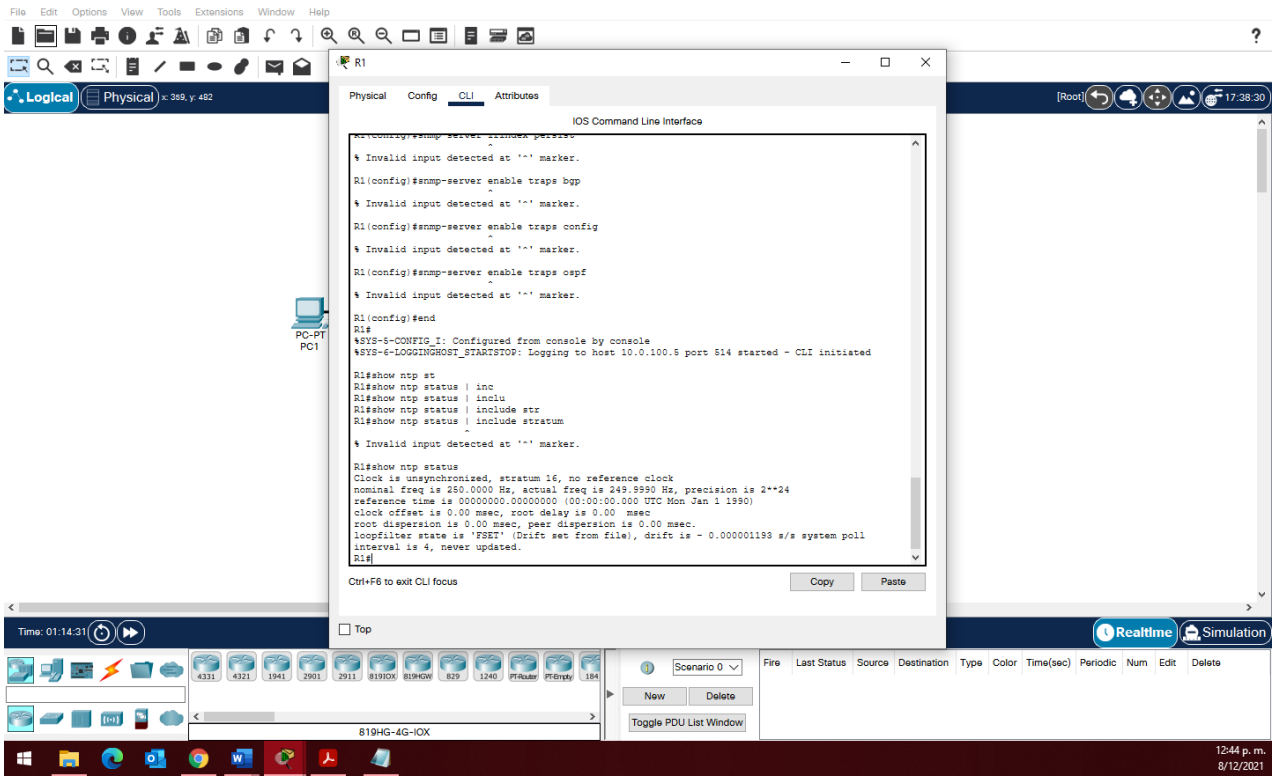


Figura 86 Validación NTP R1

VALIDACION ESTADO DE REGISTRO SYSLOG EN R1

Comando utilizado: show run | include logging

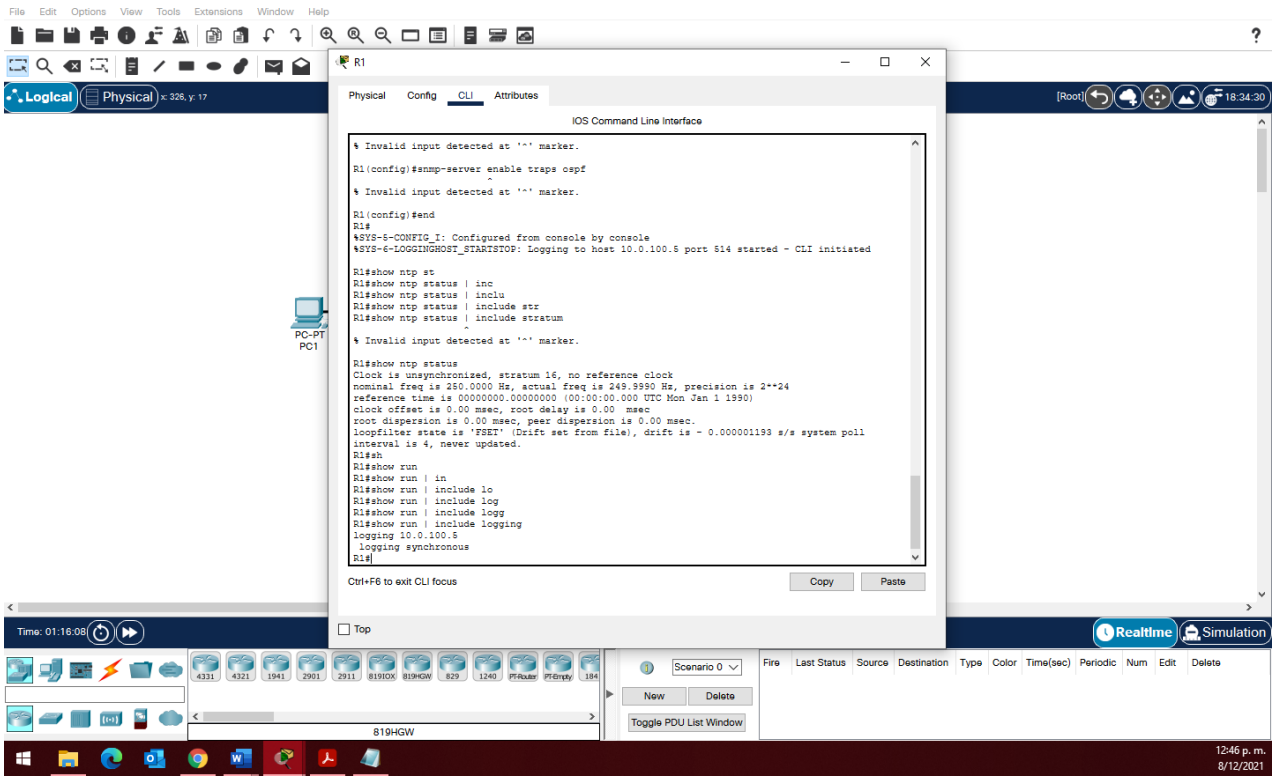


Figura 87 Syslog R1

Configuraciones en R3

Comandos utilizados:

enable

config t

ntp server 10.0.10.1

logging trap warning

logging host 10.0.100.5

logging on

ip access-list standard SNMP-NMS

permit host 10.0.100.5

exit

VALIDACIÓN SINCRONIZACIÓN NTP EN R3

Comando utilizado: show ntp status | include stratum

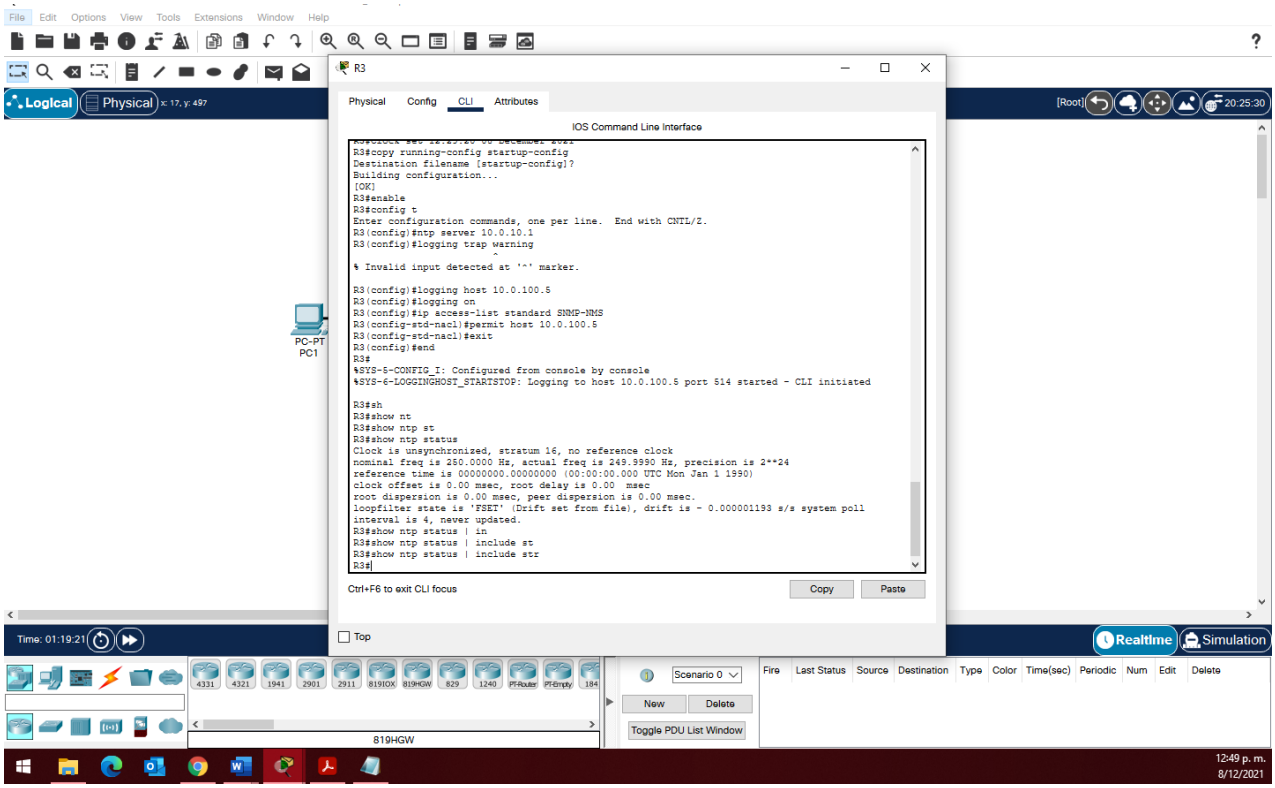


Figura 88 Sincronización NTP R3

VALIDACIÓN ESTADO DE REGISTRO SYSLOG EN R3

Comando utilizado: show run | include logging

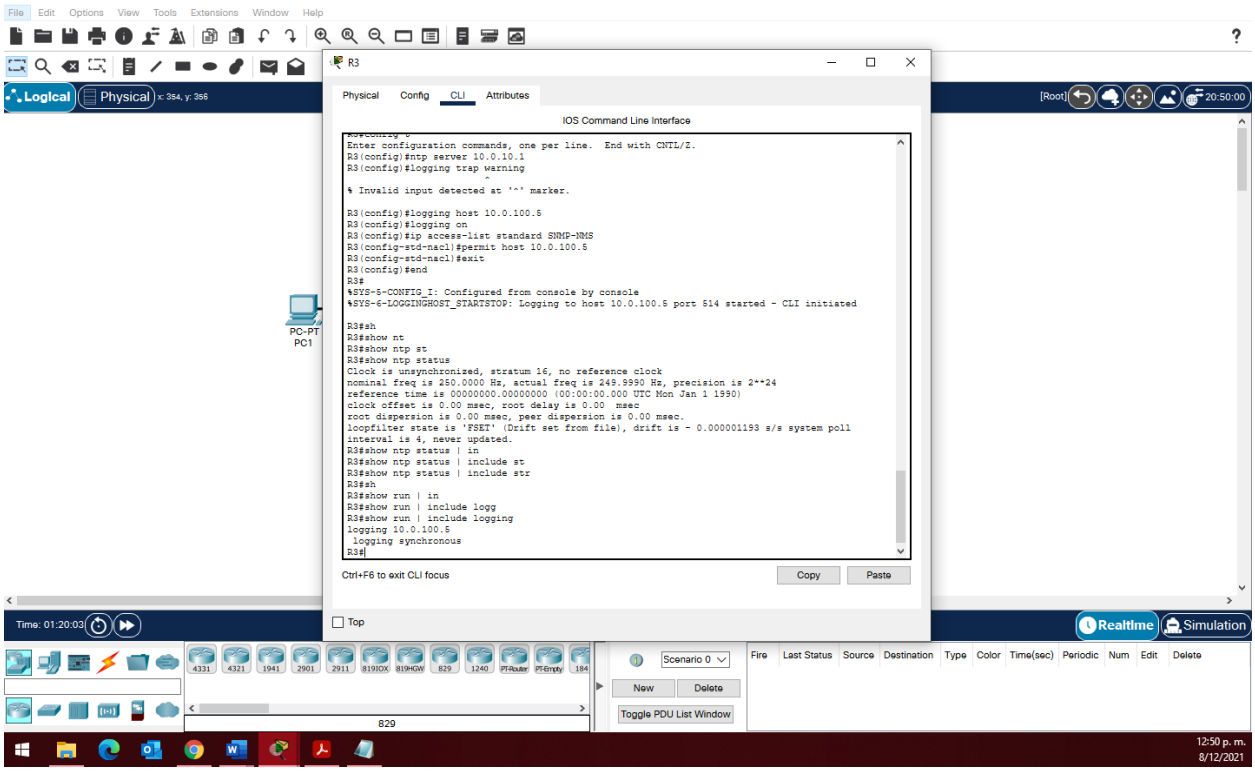


Figura 89 Syslog R3

Configuraciones en D1

Comandos utilizados:

enable

config t

ntp server 10.0.10.1 logging
trap warning logging host
10.0.100.5logging on

ip access-list standard SNMP-NMSpermit
host 10.0.100.5

exit

Configuraciones en D2

Comandos utilizados:

enable

config t

ntp server 10.0.10.1 logging
trap warning logging host
10.0.100.5logging on

ip access-list standard SNMP-NMSpermit
host 10.0.100.5

exit

VALIDACIÓN ESTADO DE REGISTRO SYSLOG EN D2

Comando utilizado: show run | include logging

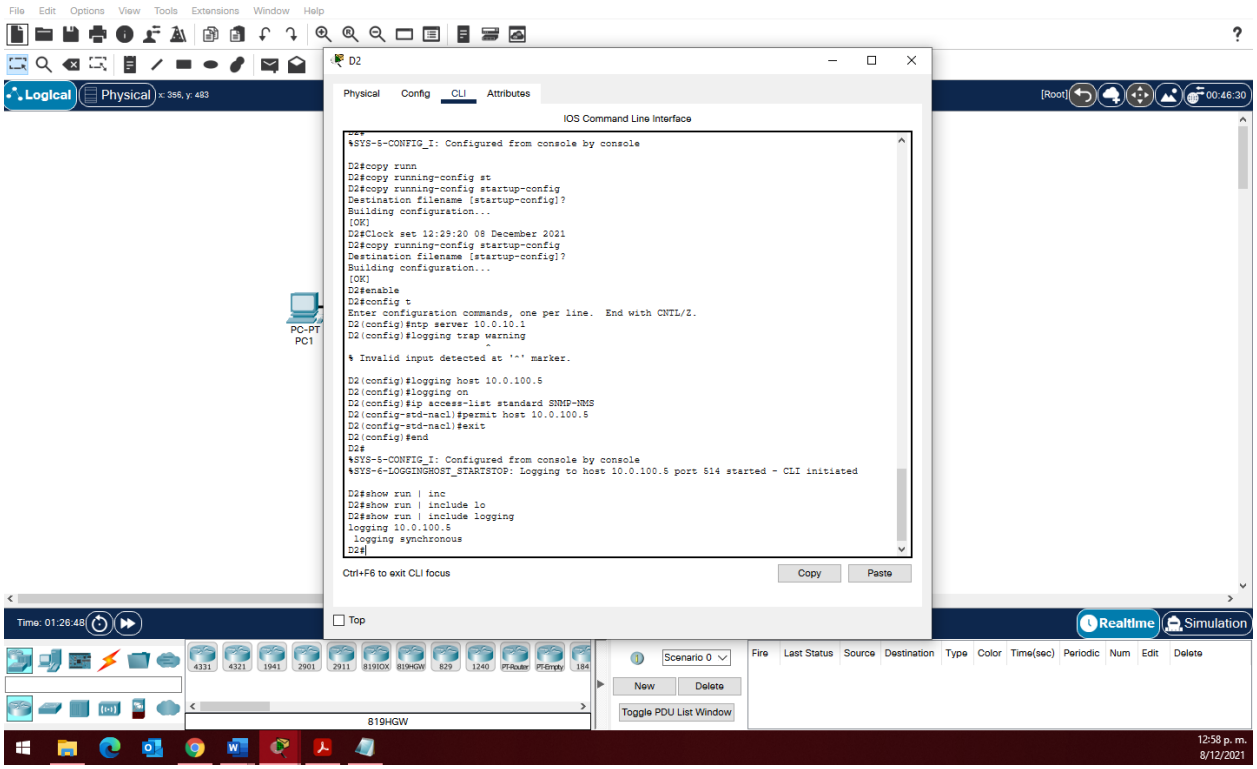


Figura 90 Syslog D2

Configuraciones en A1

Comandos utilizados:

enable

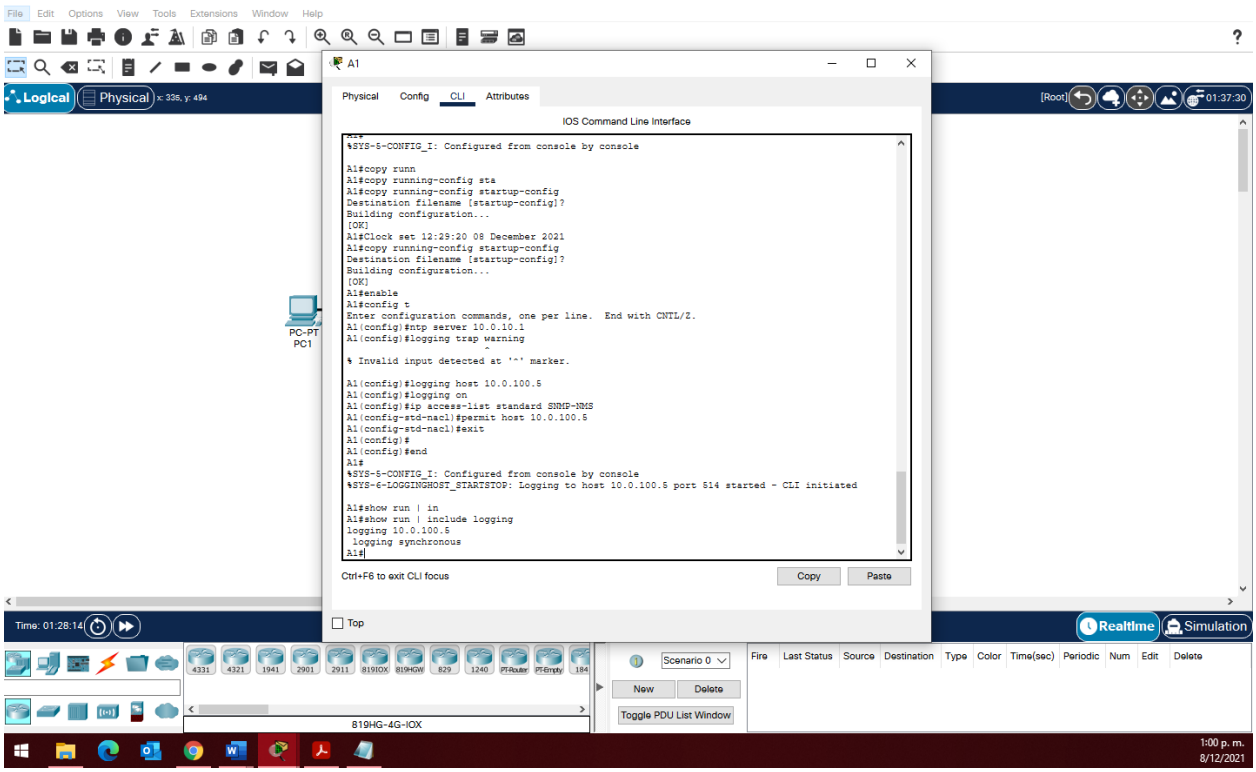
config t

ntp server 10.0.10.1 logging
trap warning logging host
10.0.100.5logging on

ip access-list standard SNMP-NMSpermit
host 10.0.100.5

exit

VALIDACIÓN ESTADO DE REGISTRO SYSLOG EN A1



Comando utilizado: show run | include logging

Figura 91 Syslog A1

CONCLUSIONES

Con todo esto el proyecto de grado que busca implementar un programa para que te dice y la instalación de una topología de red en el medio de los conceptos abordados en el diplomado de Cisco para la configuración de Router switch Type C se logra desarrollar una investigación con detalle que resuelve la problemática en determinado instante Asimismo en el transcurso de este curso se aprendió a identificar ciertos comandos como a programas y parámetros que permiten realizar un una articulación de redes en diferente punto gracias a cada uno de los programas que se han implementado de este modo logramos fortalecer nuestro conocimiento para futuros encuentros profesionales.

En esta práctica se logra habilitar OSPFv3 en los dispositivos activos de red donde se debe configurar primero una dirección ip para la habilitación del protocolo, Con la simulación de Packet Tracert se logra evidenciar que se debe llevar un orden de configuración y en el campo de trabajo ya que esto puede evitar percances o desconfiguraciones no deseadas.

Cada protocolo se logra determinar gracias a la configuración de OSPFv2 y OSPFv3 donde debe tener como referencia ya sea IPV4 e IPV6 según el caso de enrutamiento, donde los dispositivos se deben identificar y seleccionar con el fin de que soporten estos protocolos.

Gracias a la simulación realizada en Packet Tracer, y la cercanía de este programa con nuestro contexto profesional se nos permite 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.

BIBLIOGRAFIA

Dgeworth, B. Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de:https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press(Ed). Advanced Spanning Tree. CCNP and CCIE Enterprise Core ENCOR 350-401.Recuperado de: https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Understanding Wireless Roaming and Location Services. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de: https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press(Ed**).** Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de :https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press(Ed). Troubleshooting Wireless Connectivity. CCNP and CCIE Enterprise CoreENCOR 350-401. Recuperado de: https://1drv.ms/b/s!AAIGg5JUgUBthk8

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP

SWITCH 300-115. Recuperado de: https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ

The bryantadvantage.com. (2017). CCNP SWITCH Tutorial: EtherChannel Fundamentals. Recuperado de: https://www.thebryantadvantage.com/videos-and- tutorials/ccnp-switch-tshoot-tutorials/etherchannel-fundamentals/