SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JOSE ARMANDO CARDENAS MORENO

UNVERSIDAD ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS – ECBTI

INGENIERIA ELECTRONICA

IBAGUE

2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JOSE ARMANDO CARDENAS MORENO

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN Y WAN) OPCION DE GRADO

TUTOR

ING. HECTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIA - ECBTI

INGENIERIA ELECTRONICA

IBAGUE

2021

Nota de Aceptación

_____

_____

_____

_____

Presidente de jurado

_____

Jurado

_____

Jurado

Ibagué, 16 julio de 2021

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

A dios por permitirnos la salud y el entendimiento para realizar este proyecto profesional y realizar este proyecto de vida. A los tutores de la universidad nacional abierta y a distancia – unad por su dedicación, esfuerzo y el acompañamiento académico durante estos años de formación.

CONTENIDO

AGRADECIMIENTOS……4

CONTENIDO……5

LISTA DE TABLAS……..……6

LISTA DE FIGURAS……..……8

GLOSARIO……..…10

RESUMEN ABSTRACT……..……..11

INTRODUCCION……..……12

DESARROLLO……..……13

1. ESCENARIO 1……..……..13
2. ESCENARIO 2……...44

CONCLUSIONES……..82

BIBLIOGRAFIAS……..……..83

LISTA DE TABLAS

Tabla 1. Vlan……..14
Tabla 2. Asignación de direcciones……14
Tabla 3. configuración R1……18
Tabla 4. Configuración S1……..…..23
Tabla 5. Configuración S2……..……26
Tabla 6. Configuracion infraestructura (vlan, trunking, Etherchannel)……..29
Tabla 7. Configuración VLAN S2……..……..33
Tabla 8. Configuración soporte host R1……37
Tabla 9. Configuración PC-A……..……..38
Tabla 10. Configuración PC-B……..……...……....39
Tabla 11. De verificación de conectividad de la red con cada dispositivo de red……..……40
Tabla 12. Reinicio de router y switches escenario 2……43
Tabla 13. Direcciones computadora internet escenario 2……...47
Tabla 14. Configuracion R1 escenario 2……48
Tabla 15. Configuracion R2 escenario 2……50
Tabla 16. Configuraciones R3 escenario 2……53
Tabla 17. Configuracion S1 escenario 2……..……56
Tabla 18. Configuracion S3 escenario 2……57
Tabla 19. Verificación de conectividad de la red escenario 2……..……58
Tabla 20. Configuracion R1 seguridad del swtich escenario 2……..59
Tabla 21. Configuraciones S3 escenario 2……..……..61
Tabla 22. Configuraciones R1 escenario 2……..……64
Tabla 23. conectividad de la red escenario 2……..……65
Tabla 24. Configuraciones ospf en el R1 escenario 2……..……66
Tabla 25. Configuraciones ospf en el R2 escenario 2……..……68
Tabla 26. Configuracion ospf en R3 escenario 2……..……..70

Tabla 27. Comandos de muestreo de procesos ospf escenario 2……..…….72
Tabla 28. Configuraciones R1 escenario 2…….……..73
Tabla 29. Configuraciones NAT estatica y dinámica R2 escenario 2……..……74
Tabla 30. Verificación de protocolos DHCP y NAT…….…….76
Tabla 31. Configuracion NAT……..78
Tabla 32. Restricción de accesos líneas vty R2…….……..79
Tabla 33. Comandos de muestreo de ACL y NAT……..……80

LISTA DE FIGURA

Figura 1. Escenario 1 propuesto……..……..13
Figura 2. Escenario 1 simulador packet tracer…….……13
Figura 3. Plantilla sdm predeterminada S1…….……..17
Figura 4. Plantila sdm predeterminada S2……..……18
Figura 5. Puertos asignados de la interface gigabitethernet0/1 y subinterfaces….23
Figura 6. Show ip interface brief para S1……..26
Figura 7. Show ip interface brief para S2……..29
Figura 8. Show vlan S1…….……..……33
Figura 9. show vlan S2……..……..36
Figura 10. Configuración de las IP de PC-A.…….……39
Figura 11. Configuración de la IP de PC-B…….…..40
Figura 12. Ping R1 G0/2,3,4 PC-A.…….……42
Figura 13. Ping S1 y S2 VLAN 4, R1 bucle0 PC-A.……..……42
Figura 14. ping R1 G0/2,3,4 R1 Bucle0 PC-B.…….……43
Figura 15. Ping S1 y S2 VLAN PC-B…….43
Figura 16. Topologia escenario 2……..…….……44
Figura 17. Escenario 2 de la red en packet tracer de cisco……..……45
Figura 18. Show flash switches…….……..46
Figura 19. Asignación de direcciones servidor de internet.……47
Figura 20. Show interface R1……..49
Figura 21. Show interface R2……..……..……53
Figura 22. Show interface R3…….……55
Figura 23. Verificación de conectividad de la red…….……...58
Figura 24. Apagado de puertos…….……60
Figura 25. Vlan activas…….……61
Figura 26. Vlan activas S3……..……63

Figura 27. Apagado de puertos sin uso S3……...63
Figura 28. Resultados de los ping……..66
Figura 29. Ospf R1……..……..67
Figura 30. Protocolos ospf R1……68
Figura 31. Ospf R2……69
Figura 32. Protocolos ospf R2……..……...70
Figura 33. Rutas ospf R3……..……71
Figura 34. Configuraciones ospf R3……..……72
Figura 35. Configuración R1 dhcp……..……74
Figura 36. Información IP del servidor DHCP PC-A……..……77
Figura 37. Información IP del servidor DHCP PC-C……..……77
Figura 38. Ping PC-A a PC-C……..78
Figura 39. Configuración NAT……...……79
Figura 40. Interfaces R2……..……..81
Figura 41. Traducciones NAT R2……..……81

GLOSARIO

LAN: Red de Área Local es una red que conecta ordenadores en un área predeterminada, se conectan atreves de líneas telefónicas y ondas de radio esto permite que ordenadores y estaciones de trabajo estén conectadas entre si permitiendo enviar o recibir archivos y compartir acceso a los archivos y a datos en cualquier parte de la LAN eso describe que los usuarios pueden compartir lo que esté conectado a ella.

ROUTER: Es un dispositivo que recibe y envía datos de redes informáticas, los router guían y dirigen los datos de red mediante paquetes que contiene varios tipos de datos como archivos comunicaciones y transmisiones simples como interacciones web, también es capaz de priorizar los datos y elige la mejor ruta para cada transmisión.

DHCP: (Dynamic host configuration protocol, protocolo de configuración dinámica de host) es un protocolo que permite la configuración automática de red de los host de una red TCP/IP mediante un mecanismo de cliente-servidor, esto permite que los host de una red soliciten y sean asignados direcciones ip, ademas que detecta información sobre la red a la cual esta conectados.

IPV4: (internet protocolo, version4) es una versión de dirección de protocolo de internet que admite un espacio de dirección de 32 bits. Se divide en 4 campos de 8 dígitos cada uno

IPV6: (internet protocolo version6) es una versión del protocolo de internet que admite espacio de dirección de 128 bits

RESUMEN

En la elaboración de esta práctica con la implementación de estos escenarios la cual contiene actividades desarrolladas a lo largo del diplomado de profundización CCNA que nos llevan a adquirir habilidades para dar solución a un problema o el diseño de redes utilizando tecnología cisco teniendo en cuenta las diferentes plataformas de simulación y disminuir los errores mediante las herramientas de la simulación de las diferentes redes y dispositivos existentes en el mercado, en este escenario configuramos dispositivos como router, switch y pc sus ipv4 y ipv6, también como su enrutamiento en las VLAN, DHCP, y Etherchannel.

Configuramos los dispositivos y realizamos la conectividad entre ellos por medios de ping y se verifico las direcciones configuradas entre los dispositivos.

Palabras clave: CISCO, CCNP, conmutación, redes, electrónica**.**

ABSTRACT

In the elaboration of this pactice with the implementation of these scenarios which contains activities developed throughout the CCNA deepening diploma that lead us to acquire skills to solve a problem or the design cisco technology taking into account the different simulation platforms and reduce errors through simulation tools of the different networks and devices on the market, in this scenario we configure devices such as router, switch and pc their ipv4 and ipv6, as well as their routing in the VLANs, DHCP, and Etherchannel.

We configure the devices and perform the connectivity between them by ping and the addresses configured between the devices were verified.

Keywords: CISCO, CCNP, routing, switching, networking, electronics.

INTRODUCCION

En esta actividad de pruebas de habilidades se conforma de 2 escenarios propuestos propuestos en el diplomado de profundización CCNA en este avance del primer escenario daremos solución a la construcción de la red y configurando los dispositivos mediante la simulación en el packet tracer y realizando la documentación de la evidencia mediante imágenes y tablas de direcciones, comprobando la conexión de los dispositivos.

En la realización de este ejercicio vamos a afianzar los conocimientos adquiridos en ejercicios elaborados en las otras actividades del diplomado con las herramientas y con el material de apoyo en conceptos en los diferentes módulos poder desarrollar un analizar de la red con los distintos protocolos implementados y los cambios obtenidos.

Uno de los objetivos importantes de este desarrollo de este tipo de escenarios y en este en particular tener claridad de los comportamientos de los diferentes dispositivos como switch, router, y pcs configurándolos para su conectividad en los protocolos establecidos, la creación y configuraciones de redes corporativas conformadas por router, switches, pc y servidores teniendo en cuenta los diferentes enrutamientos de las VLAN, DHCP, la conectividad IPv4 y IPv6 seguridad en los diferentes switches de los 2 escenarios, en el escenario 2 los protocolos de routing dinamico OSPF, la configuración de la NAT estática y dinámica en los routers.

DESARROLLO DE LA ACTIVIDAD

ESCENARIO 1

Figura 1. escenario 1 propuesto

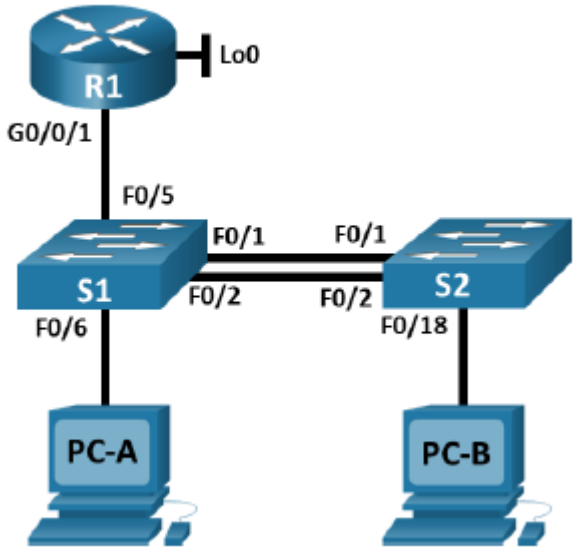
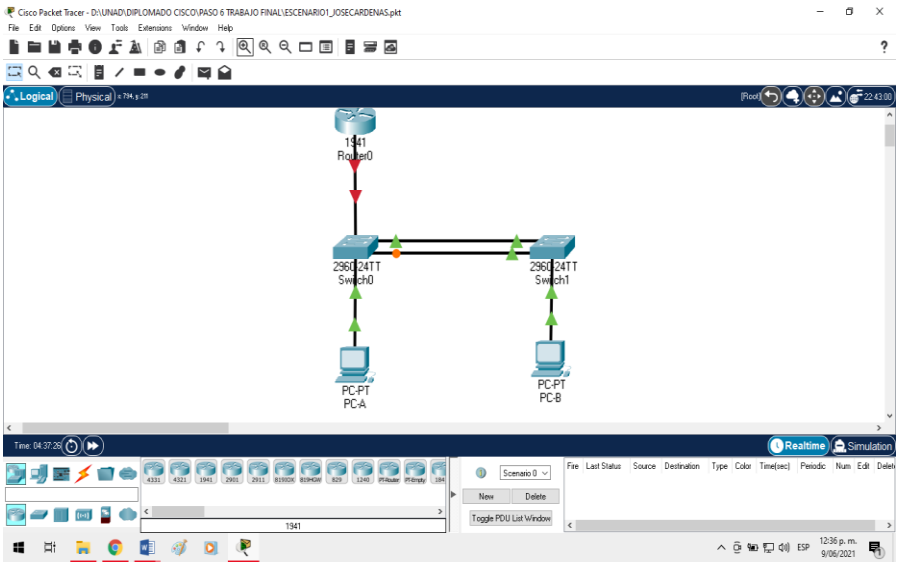


Figura 2. Figura escenario 1 simulado en packet tracer



En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conecividad IPv4 como IPv6 para los hosts soportados. El router y el switch tambien deben administarse de forma segura. Configurara el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

TABLA 1. VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

TABLA 2. DE ASIGNACION DE DIRECCIONES

DISPOSITIVO / INTERFACE	DIRECCION IP / PREFIJO	PREDETERMINADA
R1 GO/0/1.2	10.21.5.1/26 2001:db5:acad:a::1/64	No corresponde No corresponde
R1 GO/0/1.3	10.21.5.65/27 2001:db5:acad:b::1/64	No corresponde No corresponde
R1 GO/0/1.4	10.21.5.97/29 2001:db5:acad:c::1/64	No corresponde No corresponde
R1 GO/0/1.6	No corresponde	No corresponde
R1 loopback0	209.165.201.1/27 2001:db8:acad:209::1/64	No corresponde No corresponde
S1 VLAN 4	10.21.5.98/29 2001:db5:acad:c::98/64 Fe80::98	10.21.5.97 No corresponde No corresponde
S2 VLAN 4	10.21.5.99/29 2001:db5:acad:c::99/64 Fe80::99	10.21.5.97 No corresponde No corresponde
PC-A NIC	Direccion DHCP para IPv4 2001:db5:acad:a::50/64	DHCP para puerta de enlace predeterminada IPv4 Fe80::1

PC-B NIC	Direccion DHCP para IPv4 2001:db5:acad:a::50/64	DHCP para puerta de enlace predeterminada IPv4 Fe80::1

PARTE 1

INICIAR, RECARGAR Y CONFIGURAR ASPECTOS BASICOS DE LOS DISPOSITIVOS

PASO 2: INICIALIZAR Y VOLVER A CARGAR EL ROUTER Y EL SWITCH

configuraciones de inicio y la VLAN del router y del switch y vuelva a cargar los dispositivos.

El borrado de la configuración inicial del router 1 para que el dispositivo poderlo configurar de acuerdo a la red en la que vayamos a trabajar, iniciamos escogiendo el router 1941.

Configurando R1
Ingresando al CLI
Ingresando al modo privilegiado
Router>enable

Borrado de nvram
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [ok]
Erase of nvram: complete

Reiniciando el dispositivo
switch#reload
proceed with reload? [confirm] enter

configurando switch 1
ingresando al CLI
ingresando al modo previlegiado
Switch1>enable

Borrado de nvram
Switch1#erase startup-config

Erasing the nvram filesystem will remove all configuration files? Continue? [Confirm] [ok]

Reiniciando el dispositivo
Switch1#reload
Proceed with reload? [Confirm] enter

configurando switch 2

ingresando al CLI
ingresando al modo privilegiado
Switch2> enable

Borrado de nvram
Switch2#erase startup-config
Erasing the nvram filesystem will remove all configuraction files? Continue? [confirm] ok

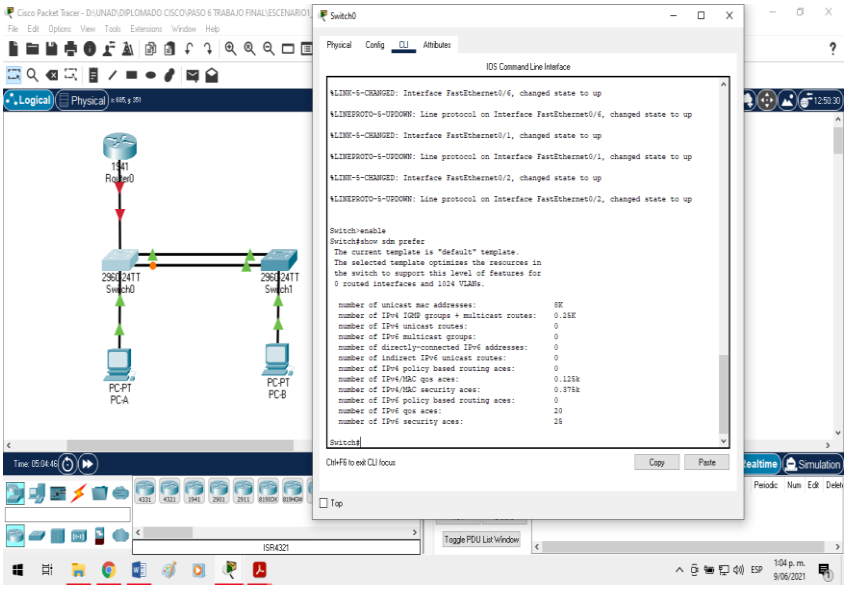
Reiniciando el dispositivo
Switch#reload
Proceed with reload? [Confirm[enter

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a recargar el switch.

Para configurar la plantilla SDM para que admita IPv6

Switch>enable - Ingresamos al modo privilegiado del switch
Switch#configure terminal - ingresa al modo de configuración
Switch(config)#show sdm prefer - muestra la plantilla predeterminada
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default - activar las preferencias de para ipv4 y ipv6
Switch(config)#exit - salimos de la configuración
Switch#reload - reiniciamos el dispositivo
Yes para guardar la modificación en el sistema y confirmar

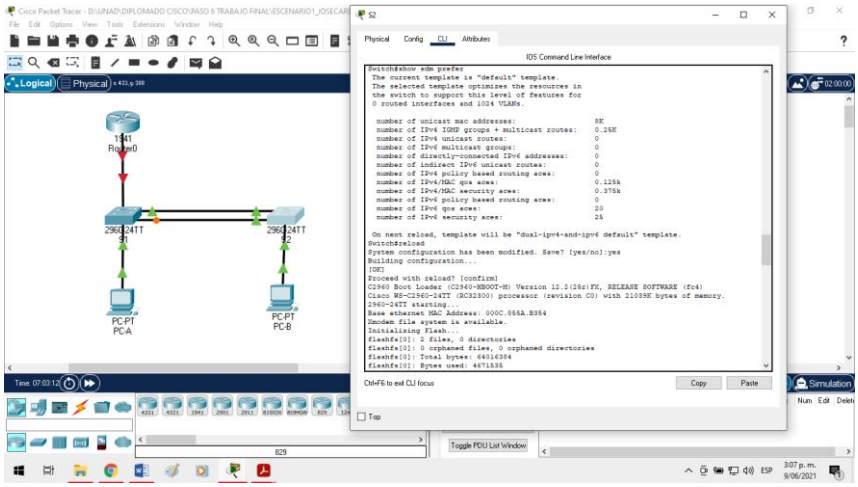
Figura 3. Plantilla SDM predeterminada S1



El switch catalist 2960 de 24 puertos ingresando en modo privilegiado
Switch2>enable
Switch2#configure terminal - ingresa al modo de configuracion

Switch2(config)#show sdm prefer - muestra la plantilla sdm (switch database manager)
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default - activa las preferencias para ipv4 y ipv6
Switch(config)#exit - para salir de la configuracion
Switch2(config)#reload - para reiniciar el dispositivo
Yes para guardar la modificación y confirmar

Figura 4. Plantilla SDM predeterminada S2



- Antes de continuar, solicite que verifique la inicialización de los dispositivos. Mediante el comando show sdm prefer se puede ver la plantilla sdm que los switch soporta ipv4 y ipv6 para la red sugerida

PASO 2: CONFIGURAR R1

Las tareas de configuración para R1 incluye las siguientes:

TABLA 3. CONFIGURACION R1

TAREA	ESPECIFICACION
Desactivar la búsqueda	desactivamos la DNS con los siguientes comandos: router>enable router#configure terminal router(config)#no ip domain lookup router(config)#end el comando **no ip domain-lookup** desactiva para evitar errores en la digitación de nombres que coincidan con comandos.

Nombre del router	Nombramos el router con los siguientes comandos: Router>enable Router#configure terminal Router(config)#hostname R1
Nombre del dominio	Para poner el nombre del dominio con los siguientes comandos: R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Para asignar la contraseña cifrada en el modo privilegiado lo haremos con las siguientes instrucciones: R1(config)#enable secret ciscoenpass R1(config)#line console 0
Contraseña de acceso a la consola	Para asignar contraseña de acceso a la consola con las siguientes instrucciones: R1(config-line)#password ciscoconpas R1(config-line)#login R1(config-line)#exit R1#
Establecer la longitud minima para las contraseñas	Para limitar la longitud minima de 10 caracteres de las contraseñas con la siguiente comando: R1(config)#security password min-length10
Crear un usuario administrativo en la base de datos local	Para crear un usuario administrativo y contaseña: Nombre de usuario. Admin Password: admin1pass el siguiente comando: R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para configurar el incio en las líneas vty para usarse en la base de datos local en el R1 con los siguientes comandos: R1(config)#line vty 0 15 R1(config-line)#login local

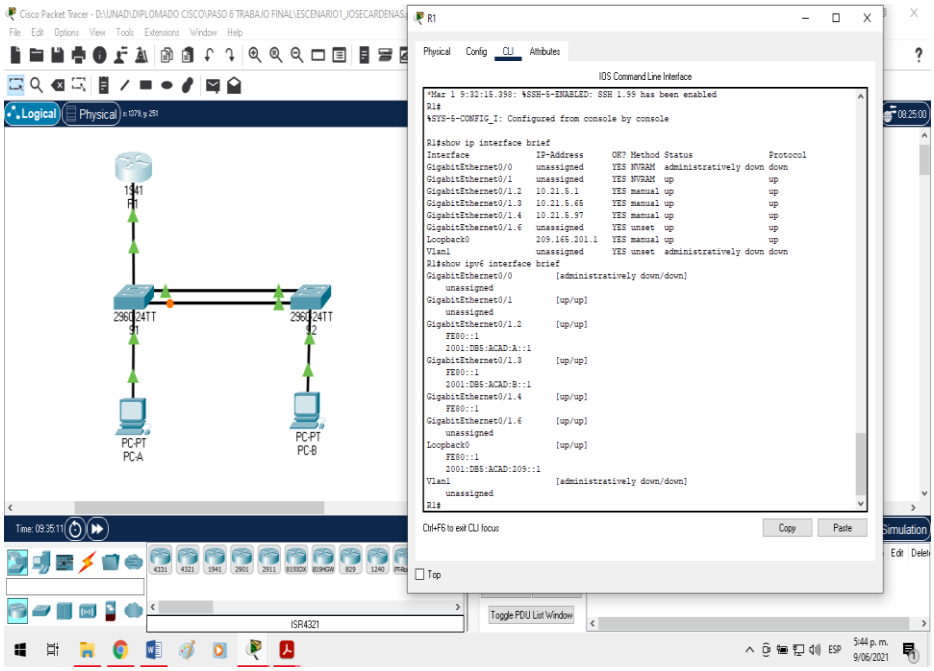
Configurar VTY solo aceptando SSH	Para configurar vty para que quede solo aceptando SSH en el R1, con las siguientes instrucciones: R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto cifrado	Para cifrar las contraseñas de texto no cifrado en el R1, con el siguiente comando: R1(config)#service password-encryption
Configure un MOTD Banner	Configurar el motd banner para poner texto que salga cuando no tiene la contraseña, R1(config)#banner motd “prohibido acceso no autorizado”
habilitar el routing IPv6	Para habilitar el routing ipv6 en el R1 Con el siguiente comando: R1(config)#ipv6 unicast-routing Con este comando ponemos en modo de configuración global habilita el routing para ipv6
Configurar interface G0/0/1 y subinterfaces	Establezca la descripción Establezca la dirección IPv4 Establezca la dirección local de enlace IPv6 como fe80::1 Establezca la dirección IPv6 Activar la interfaz Estos don los comandos para a configuración de la subinterface g0/1.2 R1(config)#interface g0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description bikes R1(config-subif)#ip address 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit Estos son los comandos para la configuración de la subinterface g0/1.3 R1(config)#interface g0/1.3 R1(config-subif)#encapsulation dot1q 3

	R1(config-subif)#description trikes R1(config-subif)#ip address 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:deb5:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit Estos son los comandos para la configuracion de subinterfaces g0/1.4 R1(config)#interface g0/1.4 R1(config-subif)#encapsilation dot1q 4 R1(config-subif)#drescription management R1(config-subif)#ip address 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#exit Estos son los comandos para la configuracion de la interface g0/1.6 R1(config)#interface g0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description native R1(config-subif)#exit Habilitar interface g0/1 R1(configure)#interface g0/1 R1(configure-if)# no shutdown R1(config)# exit Con este comando sube el Puerto gigabitethernet 0/1 lo habilita.
Configure el loopback0 interface	Establezca la descripción Establezca la dirección IPv4 Establezca la dirección local de enlace IPv6 como fe80::1

	Para configurar la interfaz loopback0 con los siguientes comandos por interfaces y subinterfaces: R1(configure)#interface loopback0 R1(configure-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db5:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#exit
Generar una clave de cifrado RSA	Para generar clave de cifrado RSA en R1 con Modulo de 1024 bits Con las siguientes instrucciones: R1(config)#crypto key generate rsa General-keys modulus 1024 Con esto ponemos el tamaño de la clave que es 1024

Finalizamos con el comando **copy running-config startup-config** para guardar la configuración y reiniciar par que queden guardadas todas configuraciónes que realizamos

Figura 5. Puertos asignados de la interface gigabitethernet 0/1 y subinterfaces



PASO 3: CONFIGURE S1 Y S2

Las tareas de configuraciones incluyen lo siguiente:

CONFIGURACION S1

TABLA 4. CONFIGURACION S1

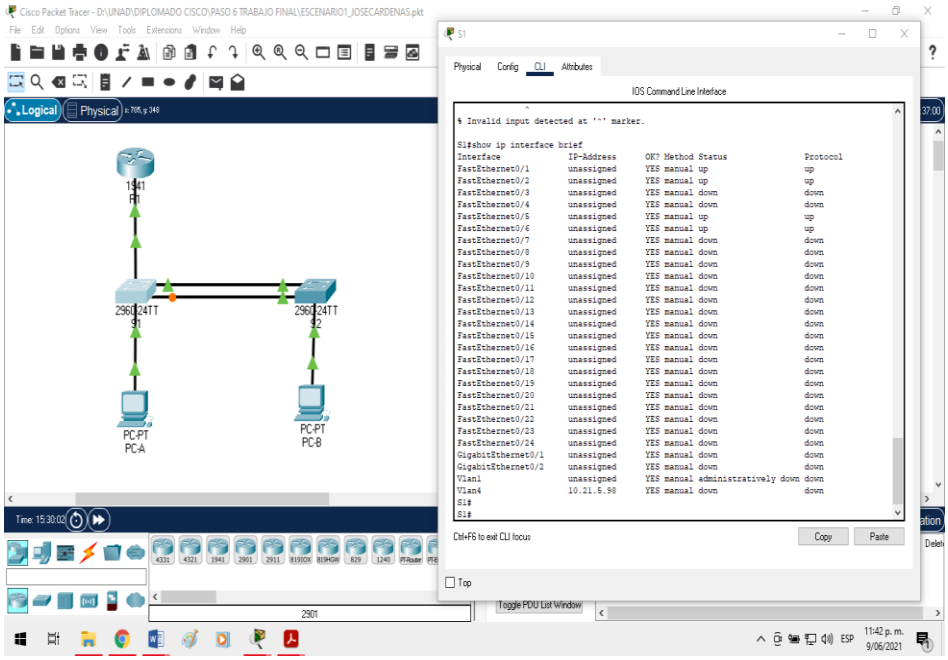
TAREA	ESPECIFICACION
Desactivar la búsqueda DNS	Desactivar la búsqueda DSN con los siguientes comandos: Switch>enable Swictch#configure terminal Switch(config)#no ip domain loopkup Switch(config)#end

	Con este comando no ip domain-loopkup desactiva para evitar error de digitación de nombres.
Nombre del switch	Para configurar el nombre del switch S1 con el siguiente comando: Switch(config)#hostname S1 S1(config)#
Nombre del dominio	para configurar el nombre de dominio del switch con el siguiente comando: s1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Para configurar la contraseña cifrada modo exec con los siguientes comandos: S1(config)#enable secret ciscoenpass S1(config)#line console 0
Contraseña de acceso a la consola	Para configurar la contraseña de la consola con el siguiente comando: S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Para crear usuario y contraseña administrativo de base de datos local con los siguientes comandos: S1(config-line)#username admin secret admin1pass S1(config-line)#exit Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para configurar el inicio de sesión en las lineas vty estos son los comandos: S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Para configurar las líneas vty para conexiones ssh estos son los comandos: S1(config-line)#transport input ssh S1(config-line)#exit

	Esto para que la autenticación sea local solo ssh
Cifrar las contraseñas de texto no cifrado.	Para cifrar texto no cifrado empleamos el siguiente comando: S1(config)#service password-encryption Aplica un cifrado debil a todas las contraseñas
Configure un MOTD Banner	Para configurar aviso de advertencia utilizamos el comando: S1(config)#banner motd “prohibido acceso autorizado”
Generar una clave de cifrado RSA	General clave cifrado RSA con el siguiente comando: S1(config)#crypto key generate rsa Generate-key modulus 1024 Con esto ponemos el tamaño de la clave 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2 Establezca la dirección IPv6 de capa 3 Para configurar la interfaz empleamos los siguiente comando: S1(config)#interface vlan S1(config-if)#description VLAN 4 S1(config-if)#ip address 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db5:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración de Gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4 utilizamos el siguiente comando:

	S1(config)#ip default-gateway 10.21.5.97 Esto para la gateway predeterminada

Figura 6.Show ip interface brief para S1



CONFIGURACION S2

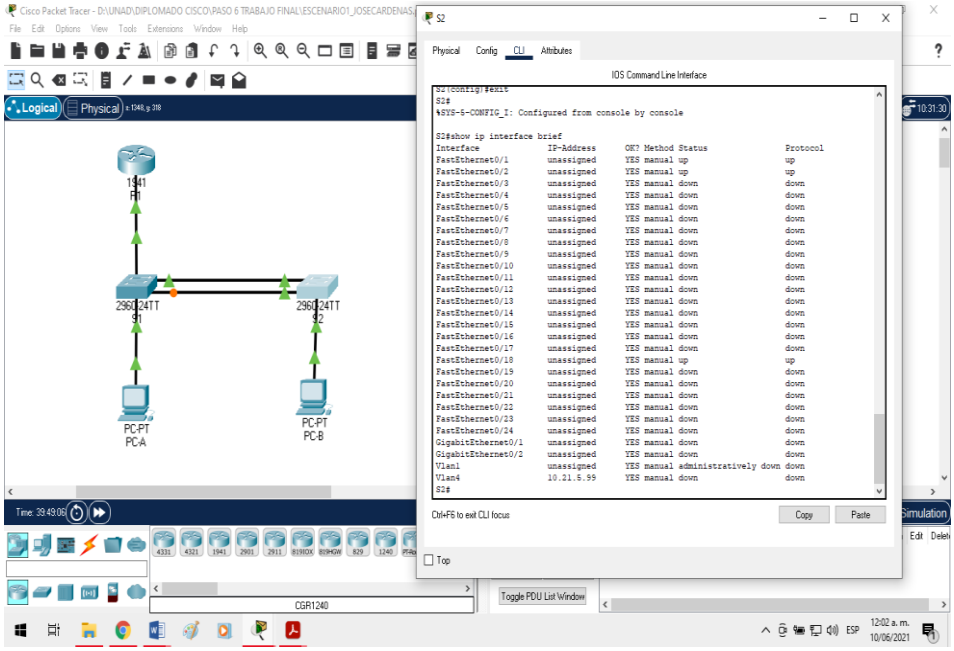
TABLA 5. CONFIGURACION S2

TAREA	ESPECIFICACION
Desactivar la búsqueda DNS	Desactivamos la búsqueda DSN con los siguientes comandos: Switch>enable Switch#configure terminal Switch(config)#no ip domain loopkup Switch(config)#end

	Con este comando no ip domain loopkup desactiva para evitar errores de digitación de nombres.
nombre del switch	Para configurar el nombre del switch S2 con el siguiente comando: Switch(config)#hostname S2 S2(config)#
nombre del dominio	Para configurar el nombre de dominio del swith con el siguiente comando: S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Pa configurar las contraseñas cifradas utilizamos el siguiente comando: S2(config)#enable secret ciscoenpass S2(config)#line console 0
Contraseña de acceso a la consola	Para configurar la contraseña de la consola utilizamos el comando: S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local	Para crear usuario y contraseña administrativo de base de datos local utilizamos el comando: S2(config-line)#username admin secret admin1pass S2(config-line)#exit Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para configurar el inicio de sesión en las líneas vty estos son los comandos: S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que la acepten únicamente la conexiones SSH	Para configurar las líneas vty para conexiones ssh estos son los comando: S2(config-line)#transport input sh S2(config-line)#exit

	Para que la autenticación sea local solo sh
Cifrar las contraseñas de texto no cifrado	Para cifrar texto no cifrado utilizamos el siguiente comando: S2(config)#service password-encryption Aplica un cifrado débil a todas las contraseñas
Configurar un motd banner	Para utilizar el aviso de emergencia utilizamos el comando: S2(config)#banner motd “prohibido acceso no autorizado”
Generar una clave de cifrado RSA	Generar clave RSA con el comando: S2(config)#crypto generate rsa Generate-key modulus 1024 Con esto ponemos el tamaño de la clave 1024bits
Configurar la interfaz de administración SVI	Establecer la dirección ipv4 de capa 3 Establecer la dirección local de enlace Ipv6 como fe80::99 Establecer la dirección ipv6 de capa 3 Para configurar la interfaz empezamos con los comandos: S2(config)# interface vlan S2(config-if)#description VLAN 4 S2(config-if)#ip address 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db5:acad:c::99/64 S2(config-if)#ipv6 address fe80::99link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuration de gateway predeterminado	Configure la puerta de enlace predeterminada como 10.21.5.97 para ipv4 utilizamos el comando: S2(config)#ip default-gateway 10.21.5.97

Figura 7. Show ip interface brief S2



PARTE 2

CONFIGURACION DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETNERNET)

PASO 4. CONFIGURACION S1

La configuración del S1 incluye las siguientes tareas:

TABLA 6. CONFIGURACION INFRAESTRUCTURA (VLAN, TRUNKING, ETHERNET)

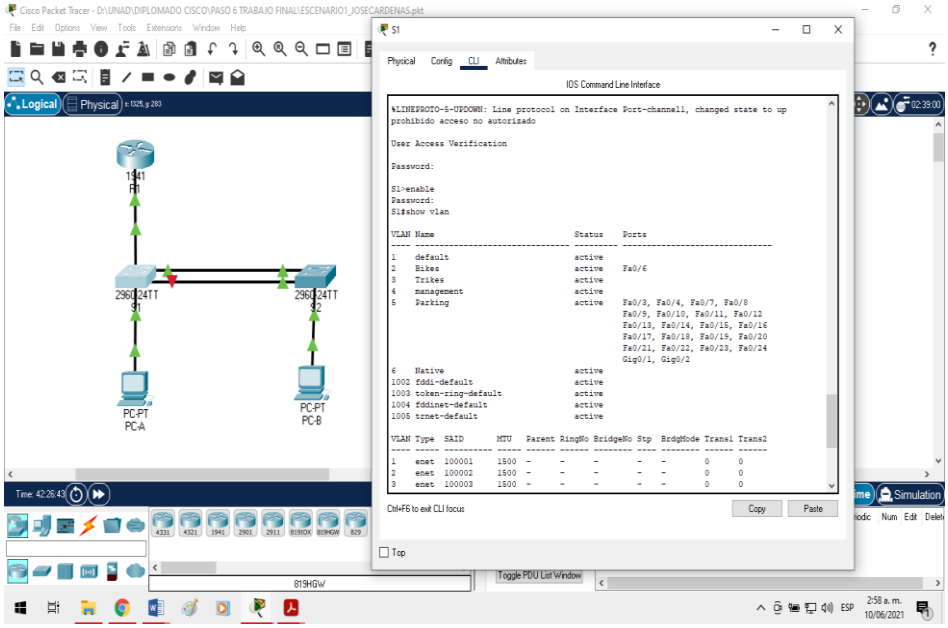
TAREA	ESPECIFICACION
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, nombre management VLAN 5, nombre parking VLAN 6, nombre nativa

	Utilizamos los siguiente comando para nombrar las vlan: S1(config)#vlan 2 S1(config-vlan)# name bikes S1(config-vlan)# exit S1(config)#vlan 3 S1(config-vlan)#name trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-valn)#name parking S1(config-valan)#exit S1(config)#vlan 6 S1(config-vlan)#name native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2, F0/5 Utilizamos los siguiente comandos para las interfaces: S1(config)#interface fa0/1 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit Show f0/1 interface switchport Este commando muestra la interfaz f0/1 S1(config)#interface fa0/2 S1(config-if)#switch mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit

	Show f0/2 interface switchport Muestra la interfaz f0/2 S1(config)#interface fa0/5 S1(config-if)#switch mode trunk S1(config-if)#switch trunk native vlan 6 S1(config-if)#exit Show f0/5 interface switchport Este commando muestra la interfaz f0/5 de vlan 6
Crear un grupo de puertos Etherchannel de capa 2 que use interfaces F0/1 Y F0/2	Usar el protocolo LACP para la negociación Estos son los comandos: S1(config)#interface rangef0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#exit Esto para crear un grupo en el Etherchannel de las dos interfaces
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 Para configurar el puerto de acceso al host para vlan 2 Empleamos los siguientes comandos: S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1config-if)#exit **No shutdown** habilita el puerto
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Para configurar el puerto de acceso para máximo 3 direcciones utilizamos los comandos: S1(config)#interface f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum3 S1(config-if)#exit

proteja todas las interfaces no utilizadas	Asignar a VLAN 5, establecer en modo de acceso, agregar una descripción apagar. Para proteger todas las interfaces sin usar, utilizamos los siguientes comandos: Vamos a abreviar con un solo parámetro todas las direcciones para disminuir el proceso los 24 puertos utilizados del s1 son f0/1, f0/2, f0/5,f0/6 Los restantes son fa0/3-4, fa0/7-24, gi0/1-2 S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switch mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description puertos sin usar S1(config-if-range)#shutdown S1(config-if-range)#exit Shutdown apaga los puertos o los deshabilita

Figura 8. Show vlan s1



PASO 5. CONFIGURE EL S2

Entre las tareas de configuración de S2 se incluyen las siguientes:

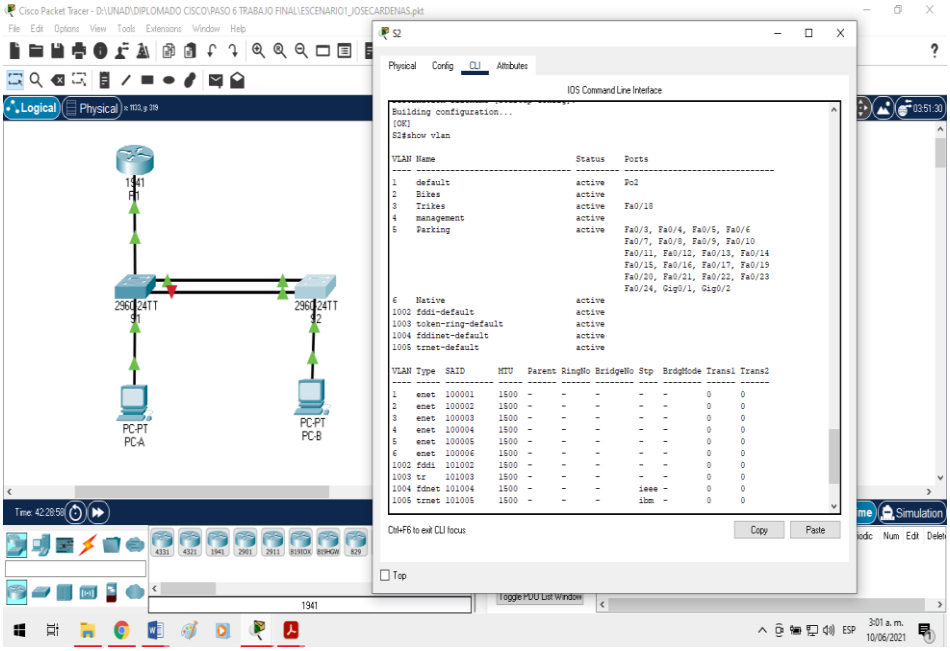
TABLA 7. CONFIGURACIÓN VLAN S2

TAREA	ESPECIFICACION
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, nombre management VLAN 5, nombre parking VLAN 6, nombre nativa Utilizamos los siguientes comandos para nombrar las vlan: S2(config)#vlan 2 S2(config-vlan)#name bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name trikes S2(config-vlan)#exit

	S2(config)#vlan 4 S2(config-vlan)#name management S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name parking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name native S2(config-vlan)exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 Utilizamos los siguiente comandos para las troncales de vlan 6: S2(config)#interface f0/1 S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit Show interface f0/1 switchport Este comando muestra la interfaz f0/1 vlan 6 S2(config)#interface f0/2 S2config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan6 S2(configure-if)#exit Show interface f0/2 switchport Este commando muestra la interfaz
Crear un grupo de puertos Etherchannel de capa 2 que use interfaces F0/1 Y F0/2	Usar el protocolo LACP para la negociación Para crear el grupo de puertos Etherchannel de la interfaces usamos los comandos: S2(config)#interface f0/1 S2(config-if)#channel-group 1 mode active S2(config-if)#exit S2(config)#interface f0/2 S2(config-if)#channel-group 1 mode active

	S2(config-if)#exit
Configurar el puerto de acceso de host para VLAN 3	Interface F0/18 Para configurar el puerto f0/18 utilizamos los siguientes comandos: S2(config)#interface f0/18 S2(config-if)#switchport mode access S2c(config-if)#switchport access vlan 3
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Configuración del puerto f0/18 utilizamos los comandos: S2(config)#interface f0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
proteja todas las interfaces no utilizadas	Asignar a VLAN 5, establecer en modo de acceso, agregar una descripción apagar. Para facilitar el ingreso de los comando y la extensión y evitar errores se trabajo se realiza en rangos de las interfaces Las interfaces utilizadas son f0/1, f0/2, f0/18 y gi0/1-2 del switch2 Las restantes de los 24 puertos del switch son f0/3-17, f0/19-24, gi0/1-2 S2(config)#interface range f0/3-17, f0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switch access vlan 5 S2(config-if-range)#Description puertos no usados S2(config-if-range)#shutdown S2(config-if-range)#exit El comando Shutdown apaga o deshabilita los puertos

Figura 9. Show vlan s2



PARTE 3

CONFIGURAR SOPORTE DE HOST

PASO 1: CONFIGURE R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 8. CONFIGURACIÓN SOPORTE HOST R1

TAREA	ESPECIFICACION
configure default routing	Crear las rutas predeterminadas para IPv4 e IPv6 que dirijan el trafico a la interfaz looback 0 Para configurar la interfaz utilizamos los comandos: R1>enable R1#configure terminal R1(config)#ip 0.0.0.0.0.0.0 loopback0 R1(config-if)#ipv6 route::/0 loopback0
Configurar IPv4 DHCP para VLAN 2	Crear un grupo DHCP para VLAN 2, compuesto por las ultimas 10 direcciones de la subred solamente. Asigne el nombre del dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Para configurar la ipv4 dhcp utilizamos loa comandos: R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#end
Configurar IPv4 DHCP para VLAN 3	Crear un grupo DHCP para VLAN 3, compuesto por las ultimas 10 direcciones de la subred solamente. Asigne el nombre del dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Para configurar la ipv4 dhcp para la vlan 3 estos son los comandos: R1(config)#ip dhcp pool vlan 3 R1(dhcp-config)#network 10.21.5.64 255.255.255.224

	R1(dhcp-config)#default-router 10.21.5.65 R1(dhcp-config)#domain-name ccna-b-b.net R1(dhcp-config)#exit

PASO 2: CONFIGURAR LOS SERVIDORES

Configure los equipos host PC – A y PC – B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y link local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

PC – A

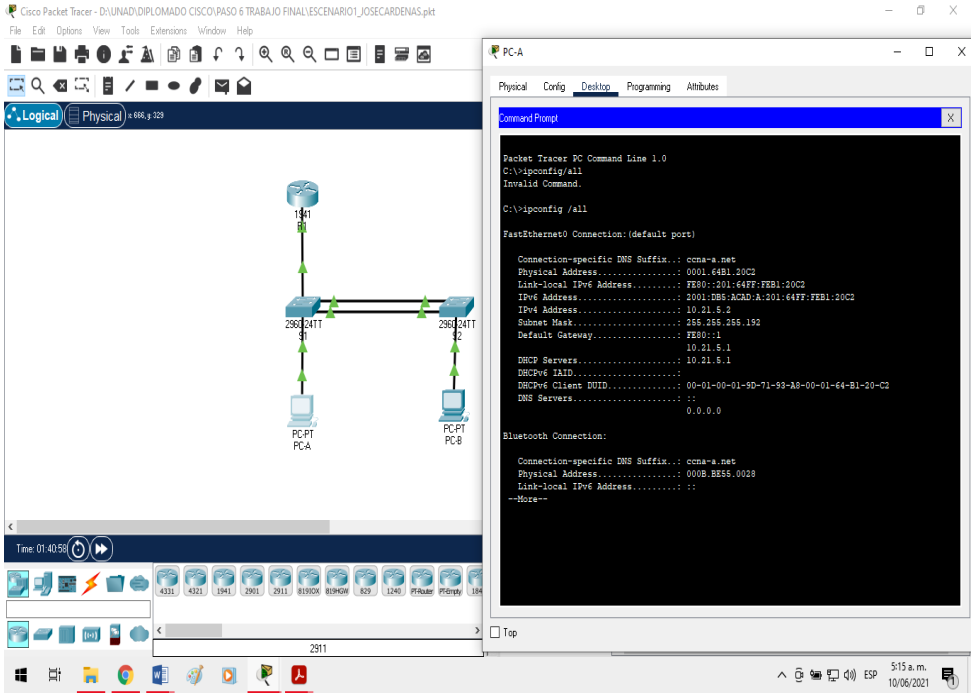
TABLA 9. CONFIGURACIÓN PC-A

CONFIGURACION DE RED PC – A	
Descripción	Ccna-a.net
Dirección física	0001.64B1.20C2
Dirección IP	10.21.5.2
Mascara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Con el comando ipconfig /all desde desktop command prompt

Configuración pc –a

figura 10. configuración de las ip del PC-A

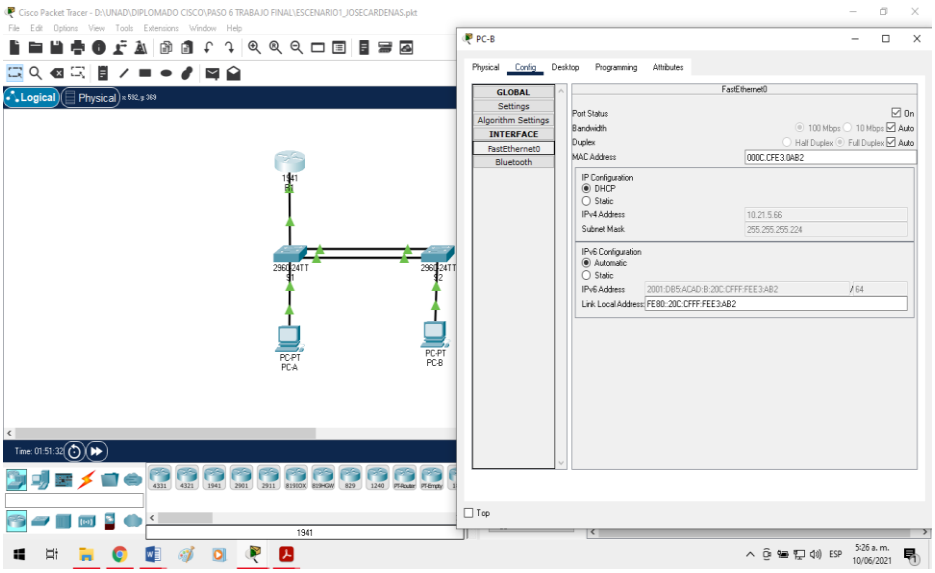


PC – B

TABLA 10. CONFIGURACIONES PC-B

CONFIGURACION DE RED PC – B	
Descripción	Ccna-b.net
Dirección física	000C.CFE3.OAB2
Dirección IP	10.21.5.66
Mascara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Figura 11. configuraciones de las ip del pc-b



PARTE 4

PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

Use el comando ping para probar la conectividad IPv4 y IPv6 entre los dispositivos de red.

TABLA 11. DE VERIFICACIÓN DE CONECTIVIDAD CON CADA DISPOSITIVO DE RED.

DESDE	A	DE INTERNET	DIRECCION IP	RESULTADOS DE PING
PC - A	R1, G0/0/1.2	Direccion	10.21.5.1	ok

		IPv6	2001:db5:acad:a::1	Ok
	R1, G0/0/1.3	Direccion	10.21.5.65	Ok
		IPv6	2001:db5:acad:b::1	Ok
	R1, G0/0/1.4	Direccion	10.21.5.97	Ok
		IPv6	2001:db5:acad:c::1	Ok
	S1, VLAN 4	Direccion	10.21.5.98	Ok
		IPv6	2001:db5:acad:a::98	Ok
	S2, VLAN 4	Direccion	10.21.5.99	Ok
		IPv6	2001:db5:acad:a::99	Ok
	PC - B	Direccion	IP address will vary	Ok
		IPv6	2001:db5:acad:b::50	Ok
	R1 bucle 0	Direccion	209.165.201.1	Ok
		IPv6	2001:db5:acad:209::1	Ok
PC - B	R1 bucle 0	Direccion	209.165.201.1	Ok
		IPv6	2001:db5:acad:209::1	Ok
	R1, G0/0/1.2	Direccion	10.21.5.1	Ok
		IPv6	2001:db5:acad:a::1	Ok
	R1, G0/0/1.3	Direccion	10.21.5.65	Ok
		IPv6	2001:db5:acad:b::1	Ok
	R1, G0/0/1.4	Direccion	10.21.5.97	Ok
		IPv6	2001:db5:acad:c::1	Ok
	S1, VLAN 4	Dirección	10.21.5.98	Ok
		IPv6	2001:db5:acad:a::98	Ok
	S2, VLAN 4	Direccion	10.21.5.99	Ok
		IPv6	2001:db5:acad:a::99	ok

Ping PC-A

Figura 12. Ping R1 G0/2,3,4

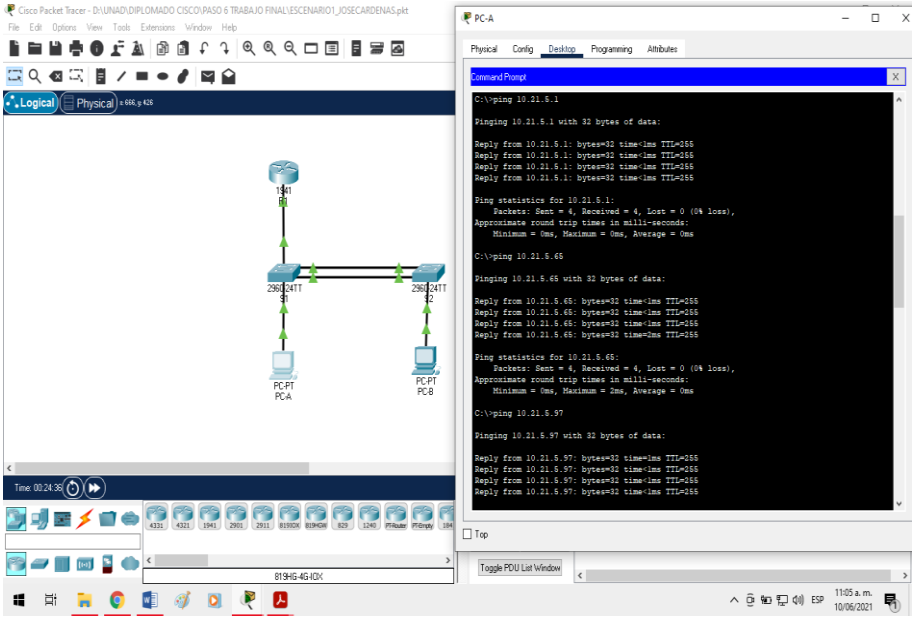
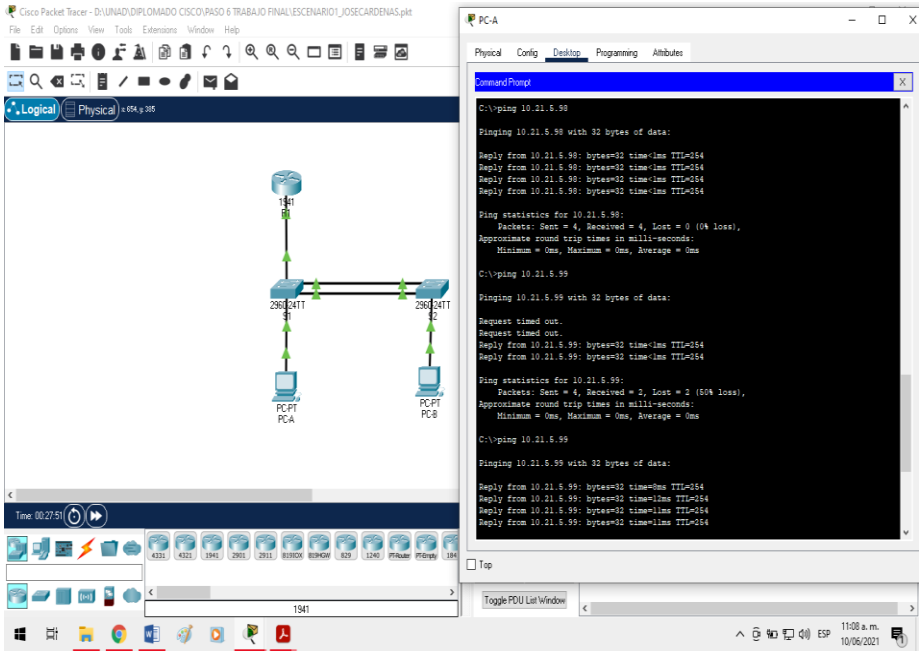


Figura 13. Ping S1 y S2 vlan4, R1 Bucle 0



ping PC-B

Figura 14. Ping R1 G0/2,3,4, R1 bucle0

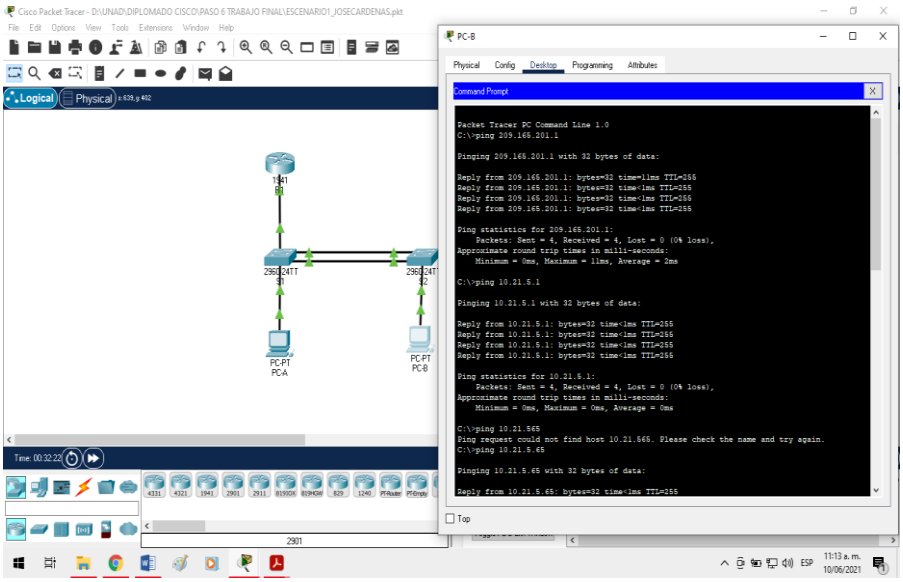
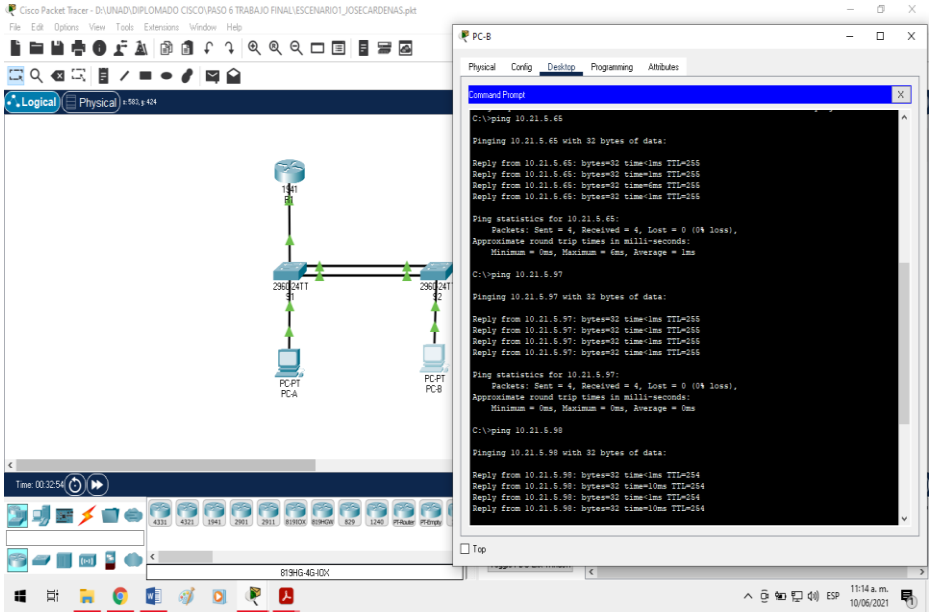


Figura 15. Ping S1 y S2 vlan4



ESCENARIO 2

Escenario: se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) sevidor/cliente. Durante la evaluación, probara y registrara la red mediante los comandos comunes de CLI.

Figura 16. topología escenario 2

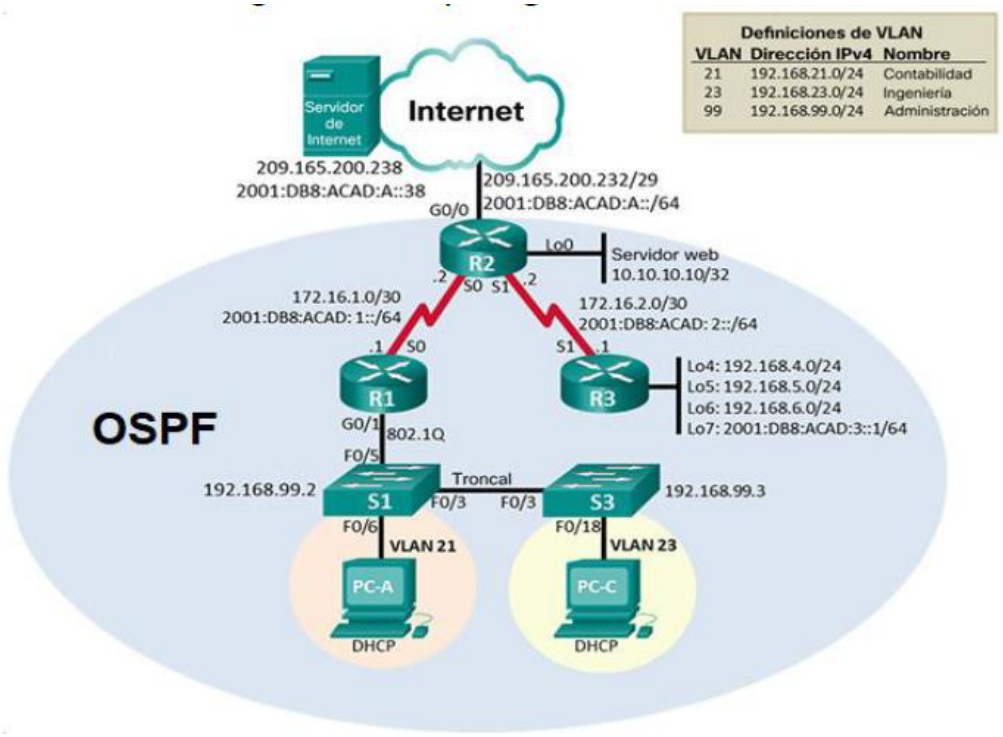
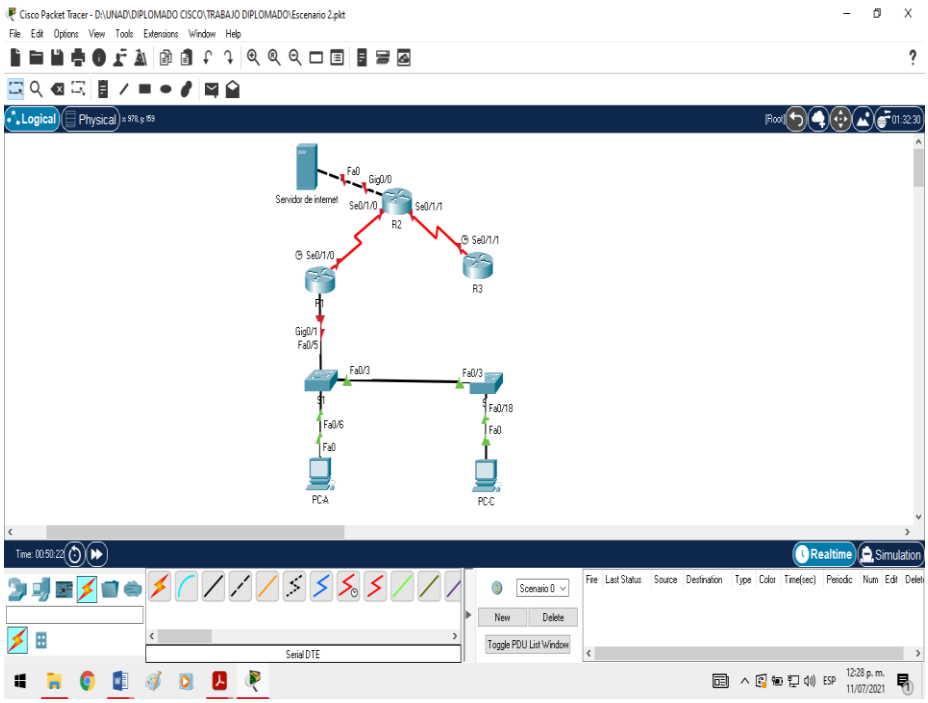


Figura 17. Escenario 2 de la red en packet tracer de cisco



PARTE 1

INICIALIZAR DISPOSITIVOS

PASO1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTER Y LOS SWITCHES

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

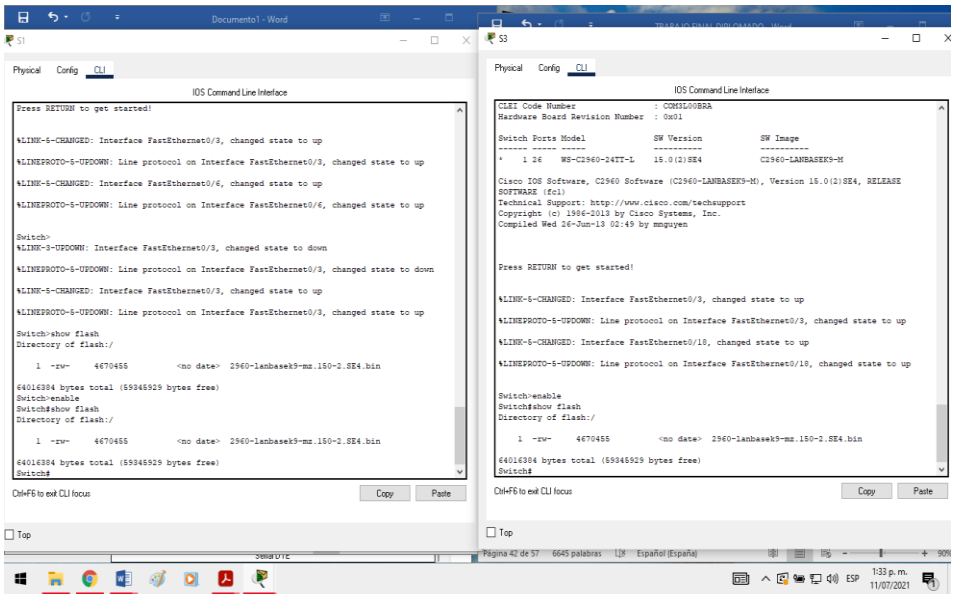
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

TABLA 12. REINICIO DE ROUTER Y SWITCHES ESCENARIO 2

TAREA	COMANDOS DE IOS
Eliminar el archivo startup-config de todos los routers	Router> enable Router#erase startup-config Este mismo comando se realiza para todos los router R1, R2, R3

Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los swtiches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Switch#detete vlan.dat Este mismo comando se realiza para todos los switches
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch# show flash

Figura 18. show flash switches



PARTE 2

CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

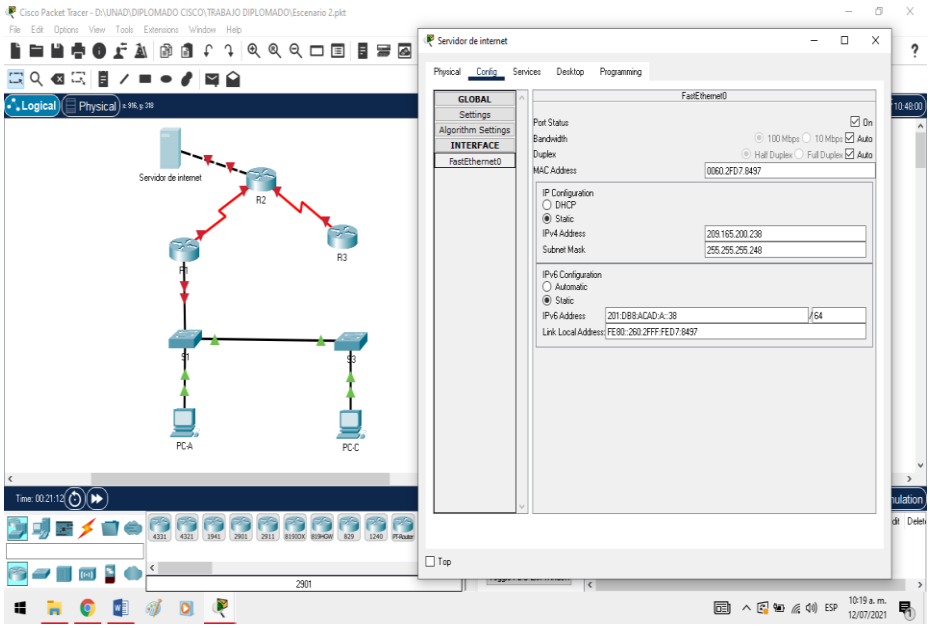
PASO1: CONFIGURAR LA COMPUTADORA DE INTERNET

Las tareas de configuración del servidor de internet incluyen lo siguiente (para obtener la información de las direcciones IP, consulte la topología):

TABLA 13. DIRECCIONES COMPUTADORA DE INTERNET ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Dirección IPv4	209.165.200.238
Mascara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/ subred	201:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Figura 19. asignación de direcciones servidor de internet



PASO 2: CONFIGURACION R1

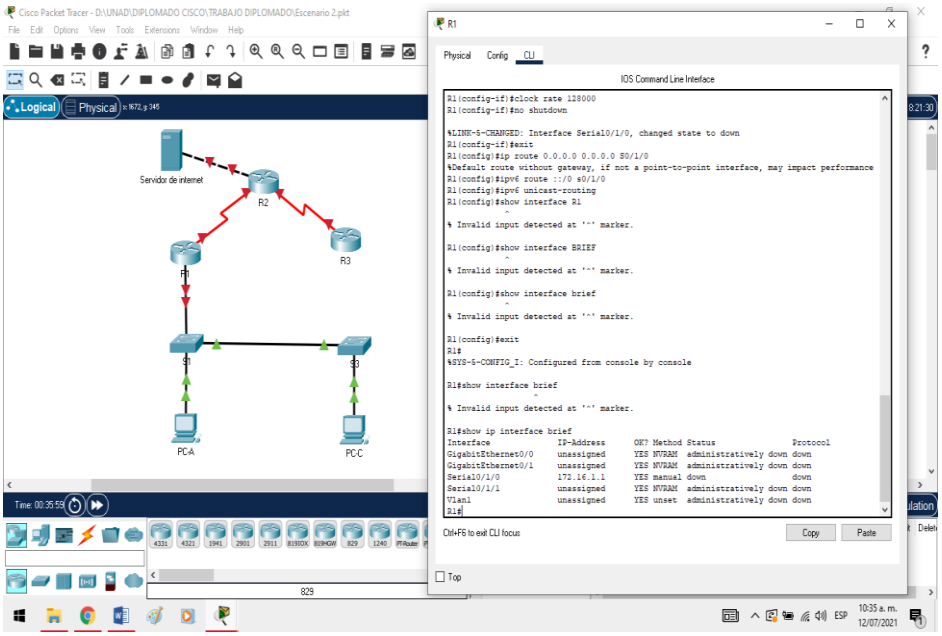
las tareas de configuración para R1 incluyen las siguientes:

TABLA 14. CONFIGURACION R1 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Desactivar la búsqueda de DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret Class
Contraseña e acceso a la consola	R1(confg)#line con 0 R1(config-line)#password cisco R1(config-line)#login R18config)-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)# banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	Establezca la descripción R1(config)#interface serial 0/1/0 R1(config-if)#description R1 a R2 Establecer la dirección IPv4 consultar el diagrama de topología para conocer la información e direcciones R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

	Establecer la frecuencia de reloj en R1(config-if)#clock rate 128000 Activar la interfaz R1(config-if)#no shutdown R1(config-if)#exit
rutas predeterminadas	Configurar una ruta IPv4 R1(config)#ip route 0.0.0.0 0.0.0.0 S0/1/0 predeterminada de S0/1/0 r1(config)#ipv6 route ::/0 s0/1/0 Configurar una ruta IPv6 R1(config)#ipv6 unicast-routing predeterminada de s0/1/0

Figura 20. Show interface R1



PASO 3: CONFIGURAR R2

La configuración de R2 incluye las siguientes tablas:

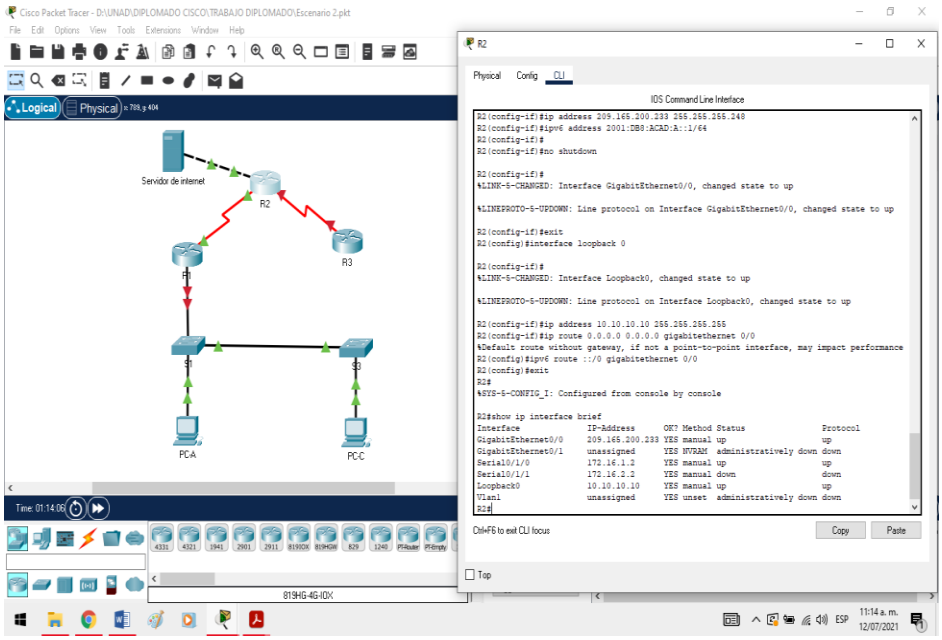
TABLA 15. CONFIGURACION R2 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
desactivar la busqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso telnet	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor de HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/0	Establezca la descripción R2(config)#interface serial 0/1/0 R2(config-if)#description R1 a R2 Establezca la dirección IPv4, utilizar la siguiente direccion disponible en la sub red. R2(config-if)#ip address 172.16.1.2 255.255.255.252

	Establezca la dirección IPv6 , consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz. R2(config-if)#c R2(config-if)#exit
Interfaz S0/0/1	Establecer la descripción R2(config)#interface serial 0/1/1 R2(config-if)#description R2 a R3 Establecer la dirección IPv4, utilizar la primera dirección disponible en la subred. R2(config-if)#ip addres 172.16.2.2 255.255.255.252 Establezca la dirección IPv6, consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Establecer la frecuencia de reloj en R2(config-if)#clock rate 128000. Activar la interfaz R2(config-if)#no shutdown R2(config -if)#exit
Interfaz G0/0 (simulación de internet)	Establecer la descripción. R2(config)#interface gigabitethernet 0/0 R2(config-if)#description R2 to internet Establecer la dirección IPv4, utilizar la primera dirección disponible en la subred. R2(config-if)#ip address 209.165.200.233 255.255.255.248

	Establecer la dirección IPv6, utilizar la primera dirección disponible en la subred R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 Activar la interfaz R2(config-if)#no shutdown R2(config-if)# exit
Interfaz loopback 0 (sevidor web simulado)	Establecer la descripción R2(config)#interface loopback 0 Establecer la direccion IPv4 R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 Predeterminada de G0/0 R2(config-if)#ip route 0.0.0.0 0.0.0.0 gigabitethernet 0/0 Configure una ruta IPv6 predeterminada de G0/0 R2(config-if)#ipv6 route ::/0 gigabitethernet 0/0 R2(config-if)#exit

Figura 21. show interface R2



PASO 4: CONFIGURACION R3

La configuración de R3 incluye las siguientes tareas:

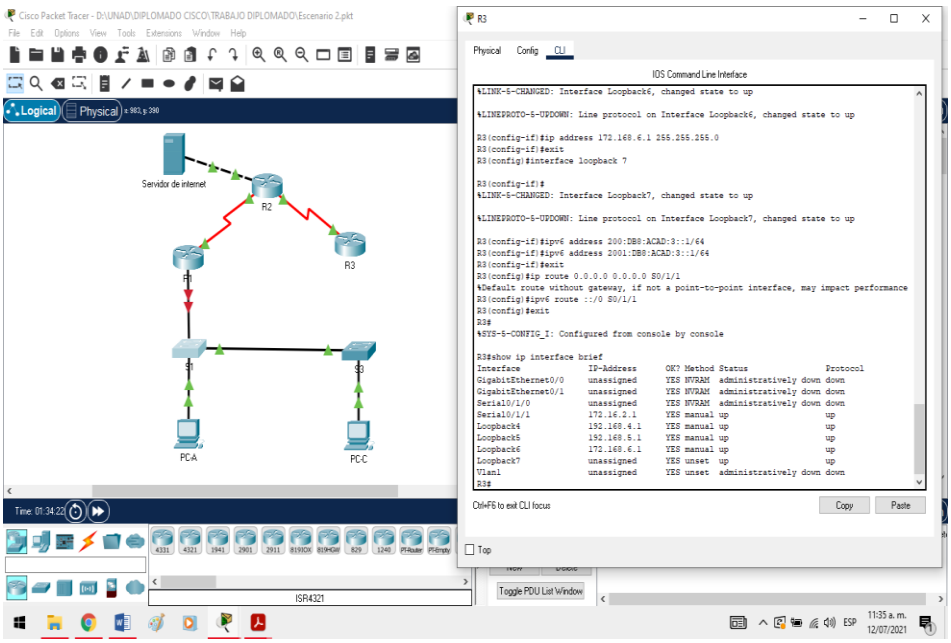
TABLA 16. CONFIGURACIONES R3 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre el router	Router(config)#hostname R3
Contraseña exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit

Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd “Se prohíbe el acceso no autorizado”
Interfaz S0/0/1	Establecer la descripción R3(config)#interface serial 0/1/1 R3(config-if)#description connection to R2 Establecer la dirección IPv4, utilizar la siguiente dirección disponible en la subred. R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6, consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 Activar la interfaz R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 4	Establezca la dirección IPv4, utilizar la primera dirección disponible de la subred R3(config)#interface loopback 4 R3 config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	establezca la dirección IPv4, utilice la primera dirección disponible de la subred. R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 6	Establezca la dirección IPv4, utilizar la primera direccion disponible de la subred. R3(config)#interface loopback 6 R3(config-if)#ip address 172.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	Establezca la dirección IPv6, consulte el diagrama de topologia para conocer la información de direcciones R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 S0/1/1 R3(config)#ipv6 route ::/0 S0/1/1

Figura 22. show interface R3



PASO 5: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

TABLA 17. CONFIGURACION S1 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Desactivar la búsqueda DNS	Switch< enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
mensaje MOTD	S1(config)#banner motd “Se prohíbe el acceso no autorizado”

PASO 6: CONFIGRACION S3

La configuración del S3 incluye las siguientes tareas:

TABLA 18. CONFIGURACIONES S3 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
nombre del switch	Switch(config)#hostname S3
Contraseña exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config)#password cisco S3(config)#login S3(config)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd “Se prohíbe el acceso no autorizado”

PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

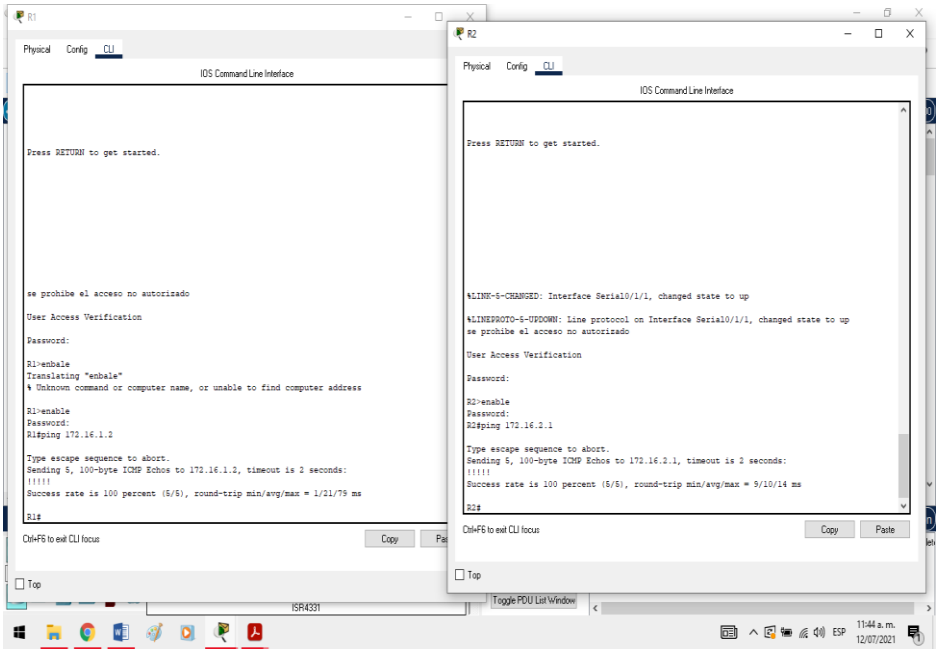
Utilice las siguientes tablas para verificar metódicamente la conectividad con cada dispositivo de red.

Tome medidas correctivas para establecer la conectividad si aluna de las pruebas falla:

TABLA 19. VERIFICACIÓN DE CONECTIVIDAD DE LA RED ESCENARIO 2

DESDE	A	DIRECCION IP	RESULTADO DEL PING
R1	R2, S0/1/0	172.16.1.2	Ok 100% (5/5)
R2	R3, s0/1/1	172.16.2.1	Ok 100% (5/5)
Pc de internet	Gateway predeterminado	209.165.200.233	Ok

Figura 23. Ping R1 a R2 y R2 a R3



PARTE 3

CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

PASO 1: CONFIGURAR S1

La configuración del S1 incluye las siguientes tareas:

TABLA 20. CONFIGURACION R1 SEGURIDAD DEL SWITCH ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para la topología para crear y nombrar cada una de las VLAN que se indican S1>enable S1#configure terminal S1(config)#vlan 21 S1(config#name contabilidad S1(config)#exit S1(config)#vlan 23 S1(config)#name ingenieria S1(config)#exit S1(config)#vlan 99 S1(config)#name adminstracion S1(config)#exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#exit Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el Gateway predeterminado	asigne la primera direccion IPv4 de la subred como el Gateway predeterminado s1(config)#ip default-gateway 192.168.99.1
Frozar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(conifg)#interface fastethernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN como VLAN nativa S1(config)#interface fastethernet 0/5

	S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface fa 0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#exit
apagar todos los puertos sin usar	S1(config)#interface range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Figura 24. apagado de puertos

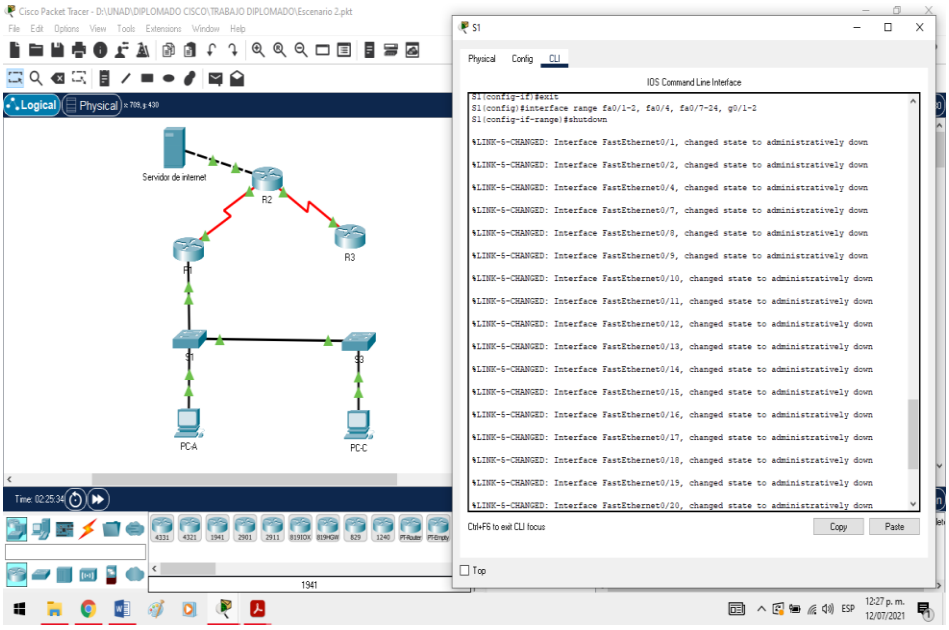
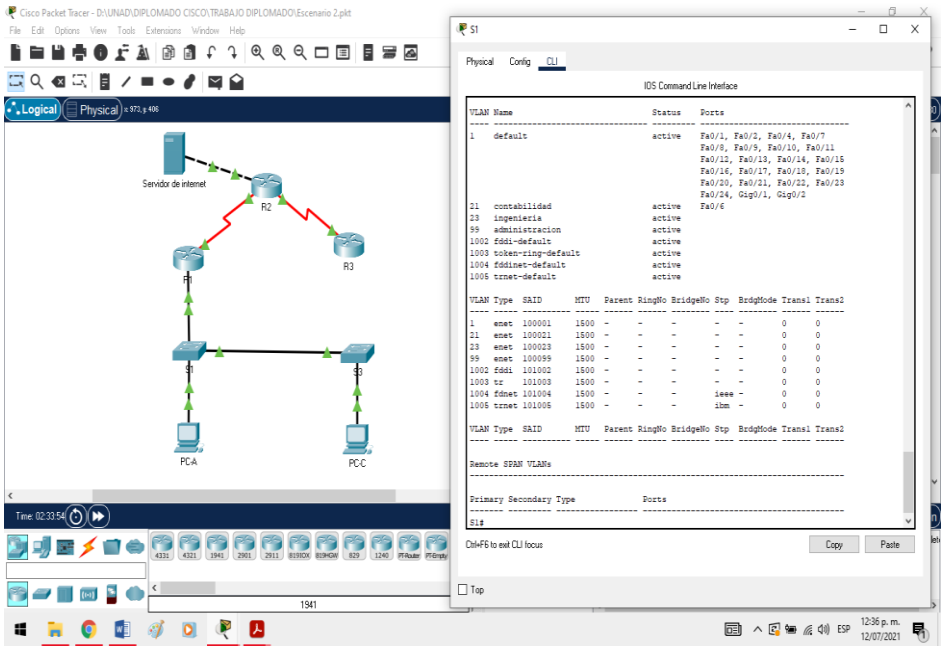


Figura 25. vlan activas



PASO 2: CONFIGURACION S3

La configuración del S3 incluye las siguientes tareas:

TABLA 21. CONFIGURACIONES S3 ESCENARIO 2

ELEMENTO O TAREA A CONFIGURAR	ESPECIFICACION
crear la base de datos de vlan	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de la VLAN que se indican de nombre a cada VLAN. S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#exit S3(config)#vlan 23

	S3(config-vlan)#name ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a las VLAN de administración. Utilizar la dirección ip asignada al S3 en el diagrama de topología S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el Gateway predeterminado	Asignar la primera dirección IP en la subred como Gateway predeterminado S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN1 como VLAN nativa S3(config)#interface fastethernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range fa0/1-2, fa0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Asignar F0/18 a VLAN 21	S3(config)#interface fastethernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
apagar todos os puertos sin usar	S3(config)#interface range fa0/1-2, fa0/4-17, fa0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Figura 26. vlan activas s3

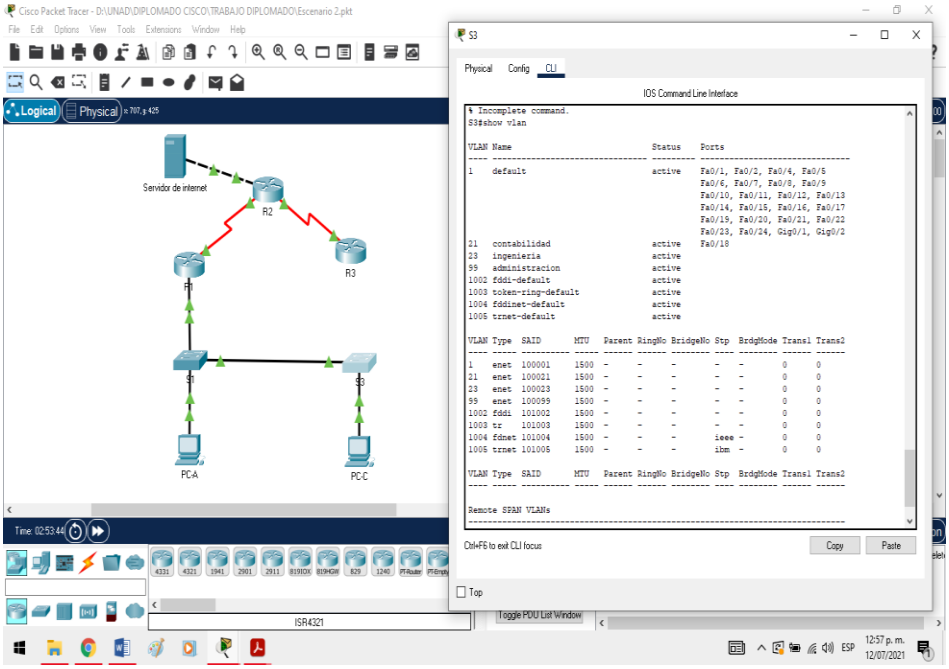
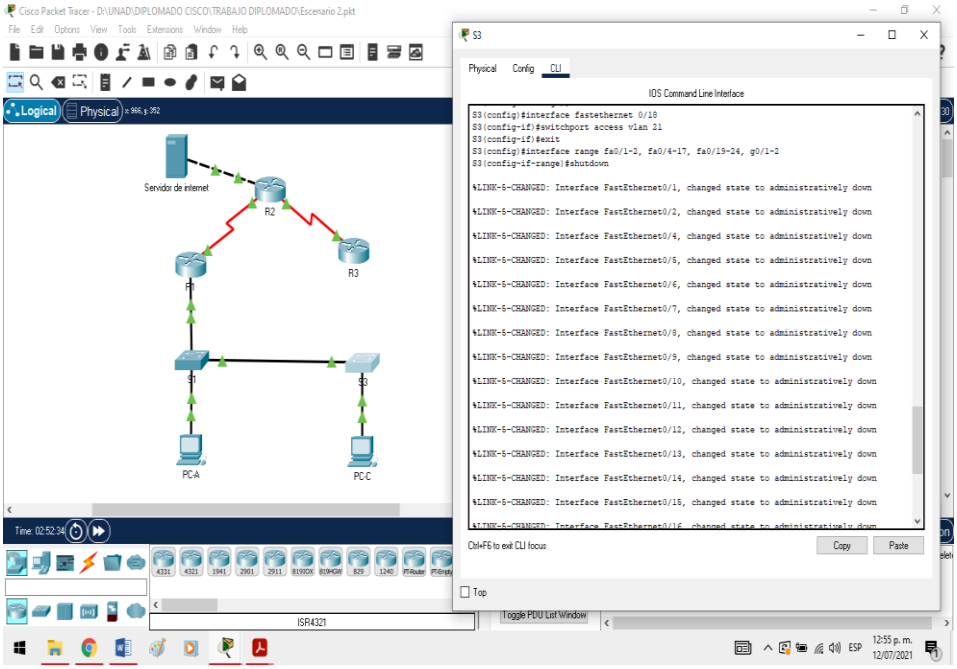


Figura 27. apagado de Puertos sin uso S3



PASO 3. CONFIGURAR R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 22. CONFIGURACIONES R1 ESCENARIO 2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
configurar la subinterfaz 802.1Q.21 en G0/1	Descripción: LAN de contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#interface gigabitethernet 0/1.21 R1(config-subif)#description accounting LAN de contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q.23 en G0/1	Descripción: LAN ingeniería Asignar la VLAN 23 R1(config)#interface gigabitethernet 0/1.23 R1(config-subif)#description accounting LAN de ingenieria R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz802.1Q.99 en G0/1	Descripción: LAN administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config)#interface gigabitethernet 0/1.99 R1(config-subif)#description accounting LAN de administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface gigabitethernet 0/1 R1(config-if)#no shutdown

	R1(config-if)#exit

PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

Utilice el comando ping para probar la conectividad entre los switches y el R1.

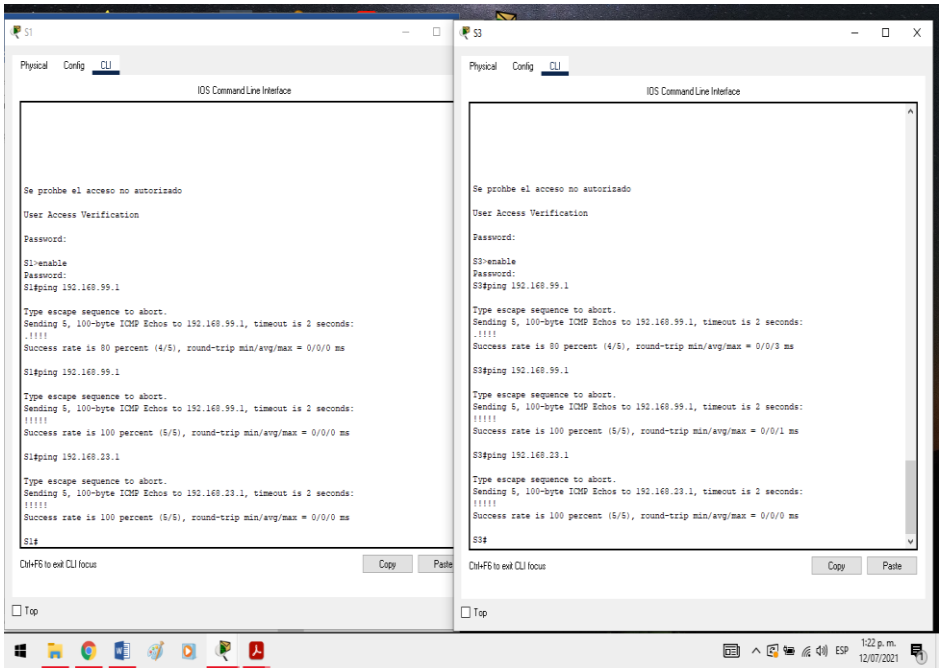
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

TABLA 23. CONECTIVIDAD DE LA RED ESCENARIO 2

DESDE	A	DIRECCION IP	RESULTADOS DE PING
S1	R1, dirección VLAN 99	192.168.99.1	Ok 100% 5/5
S3	R1, direccion VLAN 99	192.168.99.1	Ok 100% 5/5
S1	R1, direccion VLAN 21	192.168.21.1	Ok 100% 5/5
S3	R1, direccion VLAN 23	192.168.23.1	Ok 100% 5/5

Figura 28. resultado de los ping



PARTE 4

CONFIGURAR LOS PROTICOLOS DE ROUTING DINAMICO OSPF

PASO1: CONFIGURAR OSPF EN EL R1

Las tareas de configuración para R1 incluyen las siguientes:

TABLA 24. CONFIGURACIONES OSPF EN EL R1 ESCENARIO 2

TAREA O ELEMENTO DE CONFIGURACION	ESPECIFICACION
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0

anunciar la redes conectadas directamente	Asigne todas las redes conectadas directamente R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive las sumarizacion automatica	R1(config)#router rip R1(config-router)#no auto-summary

Figura 29. ospf R1

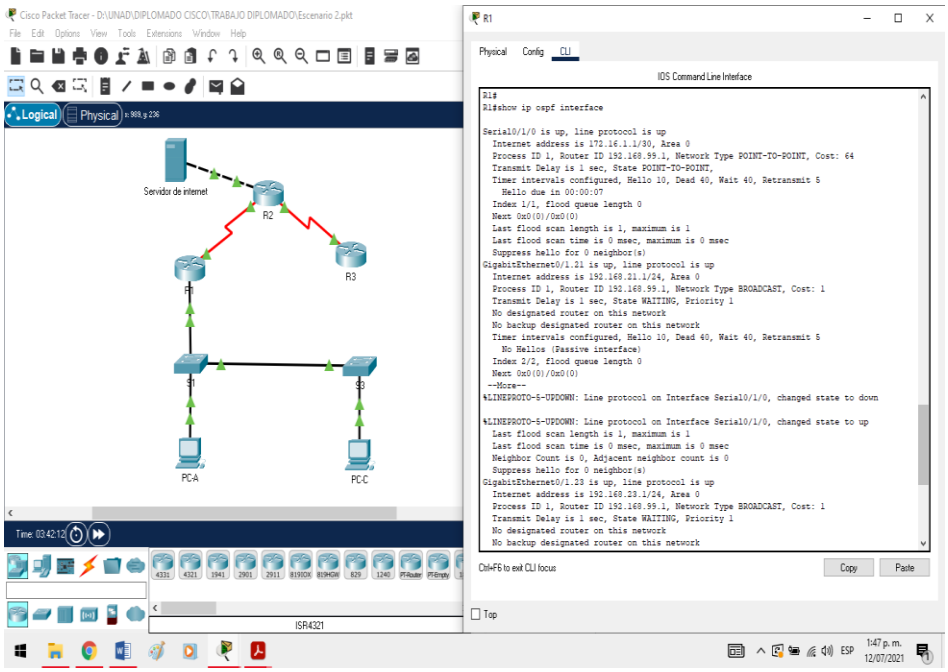
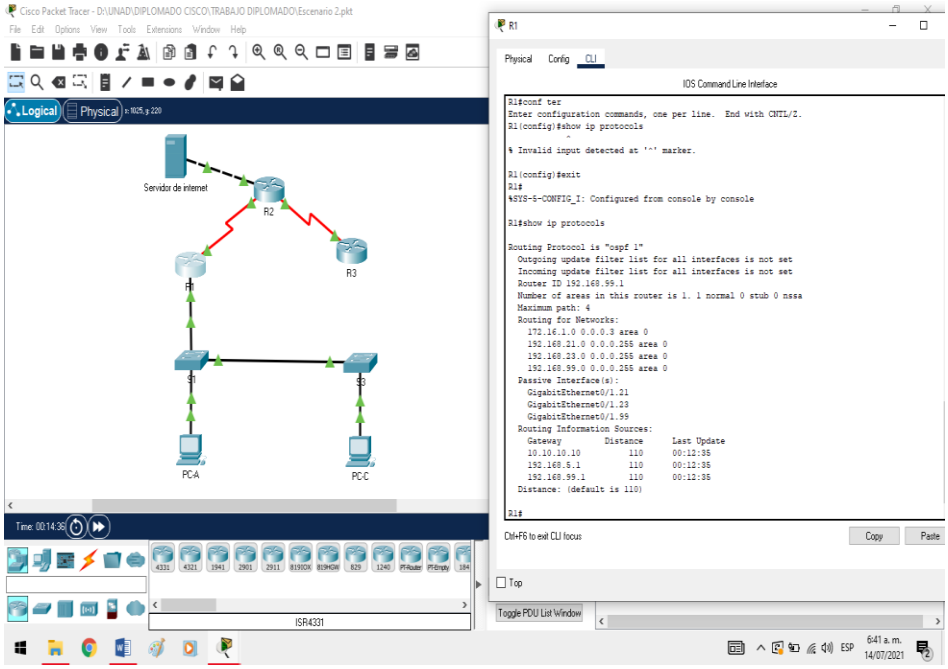


Figura 30. protocolos ospf R1



PASO 2: CONFIGURAR OSPF EN EL R2

las configuraciones del R2 incluyen las siguientes tareas:

TABLA 25. CONFIGURACIONES OSPF EN EL R2

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
configurar OSPF area 0	R2(config)#router ospf 1 R2(config-router)#network 10.10.10.10 0.0.0.3 area 0
anunciar las redes conectadas directamente	Nota. Omitir la red G0/0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0

Desactive la sumarizacion automática.	R2(config-router)#no auto-summary

Figura 31. ospf R2

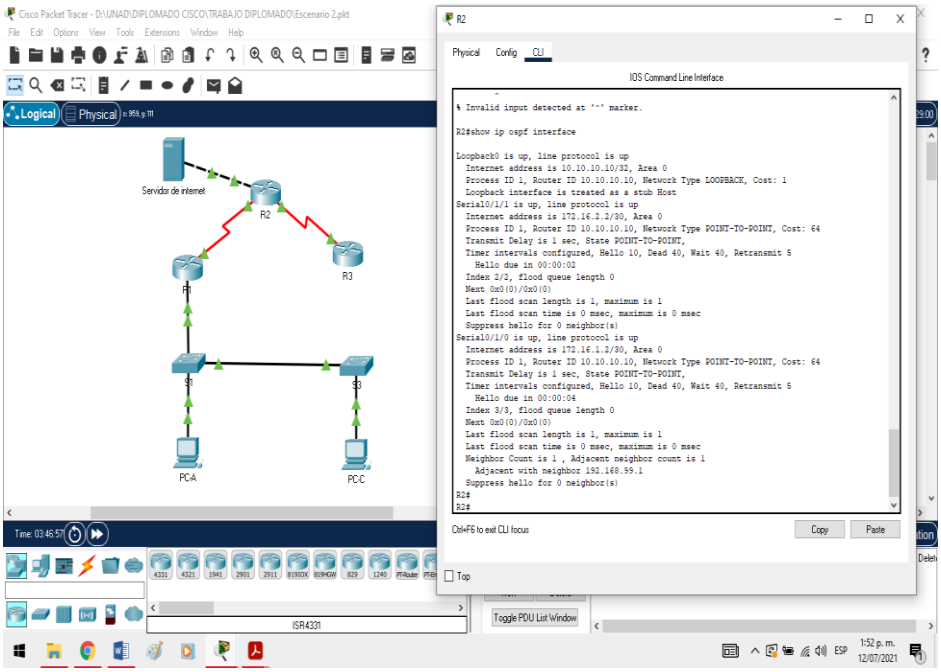
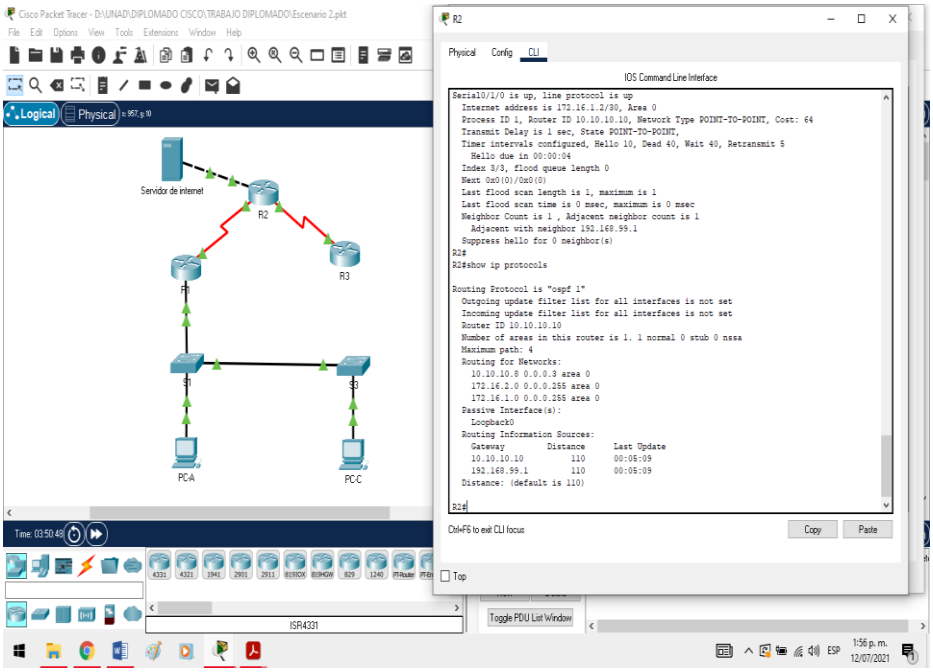


Figura 32. protocolos ospf R2



PASO 3: CONFIGURAR OSPFv3 EN EL R3

TABLA 26. CONFIGURACIÓN OSPF EN R3

ELEMENTO O TAREA DE CONFIGURACION	ESPECIFICACION
Configurar OSPF área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (loopback) como pasivas	R3(config-router)#passive-interface loopback 4

	R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarizacion automatica	R3(config-router)#no auto-summary

Figura 33. rutas ospf R3

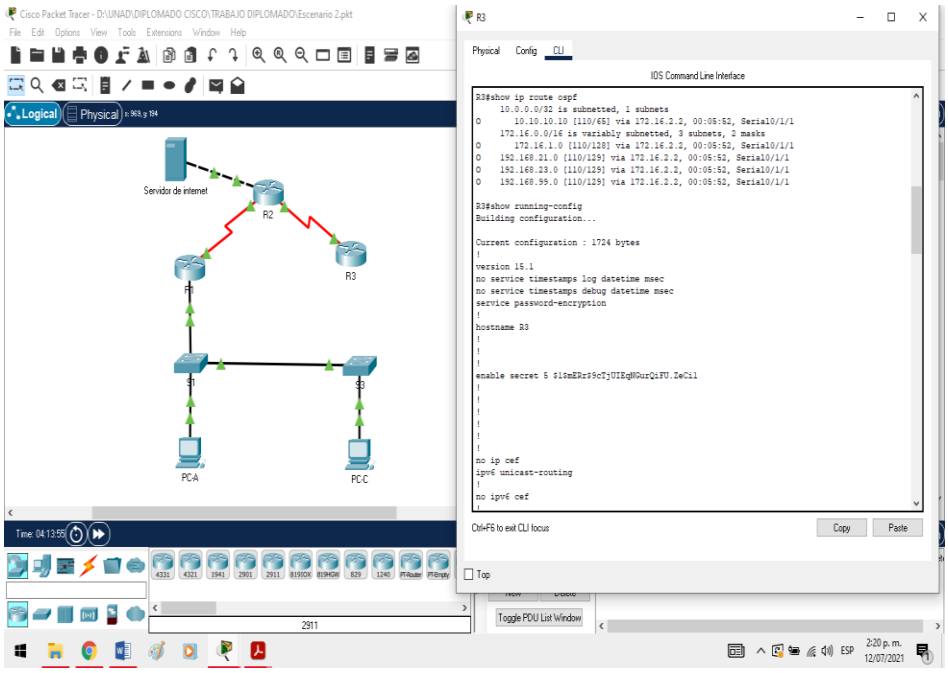
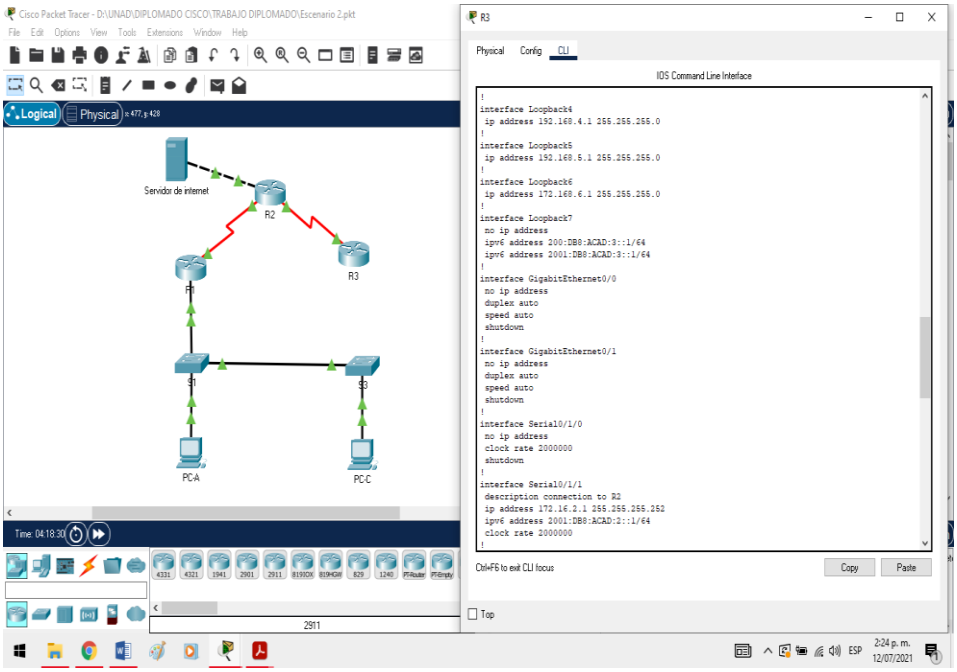


Figura 34. configuraciones ospf R3



PASO 4: VERIFICAR LA INFORMACION DE OSPF

Verifique que OSPF este funcionando como se espera, introduzca el comando de CLI adecuado para obtener la siguiente información:

TABLA 27. COMANDOS DE MUESTREO DE PROCESOS OSPF ESCENARIO 2

PREGUNTA	RESPUESTA
Con que comando se muestra la ID del proceso OSPF, la ID del router, las redes del routing y las interfaces pasivas configuradas en un router?	show ip ospf interface show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show running-config

PARTE 5

IMPLEMENTAR DHCP Y NAT PARA IPV4

PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

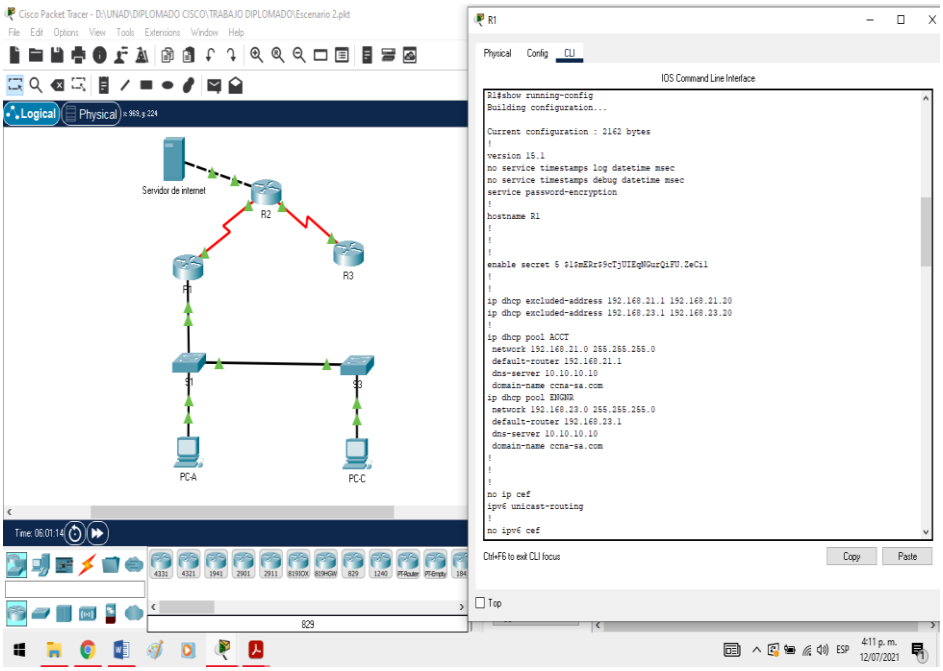
Las tareas de configuración para R1 incluyen las siguientes:

TABLA 28. CONFIGURACIONES R1 ESCENARIO 2

ELEMENTO O TAREA A CONFIGURAR	ESPECIFICACION
Reservar las primeras 20 direcciones IP en las VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21	Nombre: ACCT Servidor DNS 10.10.10.10 Nombre del dominio: ccna-sa.com Establecer el Gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre del dominio: ccna-sa.com Establecer el Gateway predeterminado R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

	R1(dhcp-config)# exit

Figura 35. configuración R1 dhcp



PASO 2: CONFIGURAR LA NAT ESTATICA Y DINAMICA EN EL R2

La configuración del R2 incluyen las siguientes tareas:

TABLA 29. CONFIGURACIONES NAT ESTATICA Y DINÁMICA R2 ESCENARIO 2

ELEMENTO O TAREA A CONFIGURAR	ESPECIFICACION
Crear una base de datos local con una cuenta de usuario	Nombre del usuario: webuser Contraseña: cisco12345 Nivel de privilegio. 15 R2>enable R2#configure terminal R2(config)#user webuser privilege 15 secret cisco 12345

Habilitar el servicio del servidor HTTP	R2(config)#ip http server No es soportado el comando
Configuar el servidor HTTP para utilizar la base de datos para la autenticacion	No soportado
Crear una NAT estatica al servidor web	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estatica	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de contabilidad y de ingeniería en el R1. Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Defina el pool de direcciones IP publicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinamica	R2(config)#ip nat inside source list 1 pool INTERNET

PASO 3: VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTATICA

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estatica funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

TABLA 30. VERIFICACION DE PROTOCOLOS DHCP Y NAT

PRUEBA	RESULTADOS
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Dirección IPV4: 192.168.21.21 Mascara subred: 255.255.255.0 Gateway predeterminado: 192.168.21.1 DNS server: 10.10.10.10
verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Dirección IPv4: 192.168.21.22 Mascara sub red: 255.255.255.0 Gateway predeterminado: 192.168.21.1 DSN server: 10.10.10.10
Verificar que la PC-A pueda hacer ping a PC-C	Ok exitoso el ping
Utilizar un navegador web en la computadora de internet para acceder al servidor web (209.165.200.229) iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	ok

Figura 36. información IP del servidor DHCP PC-A

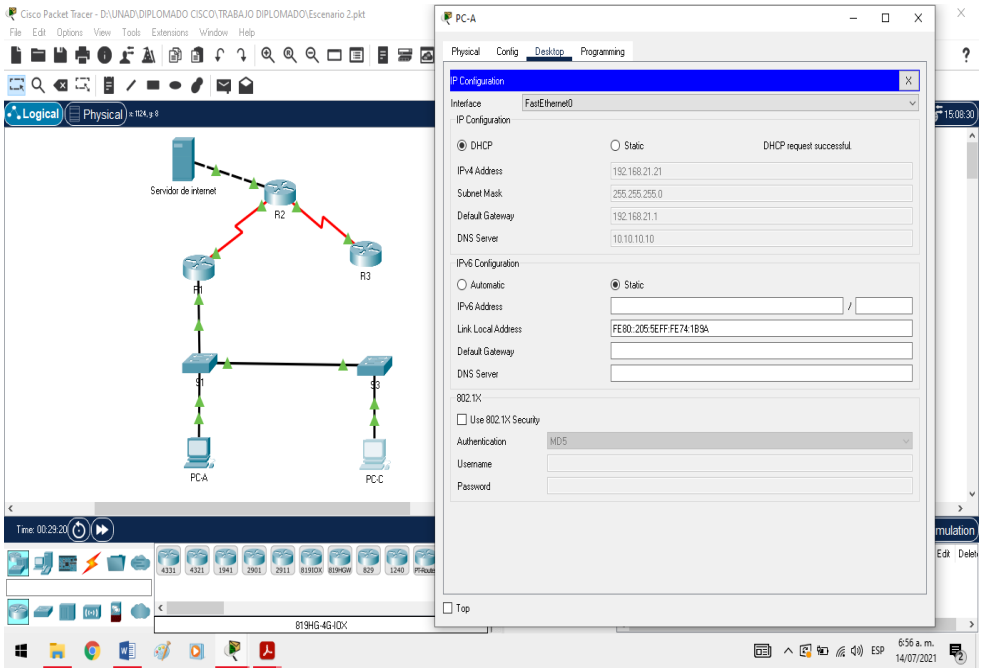


Figura 37. información IP del servidor dhcp pc-c

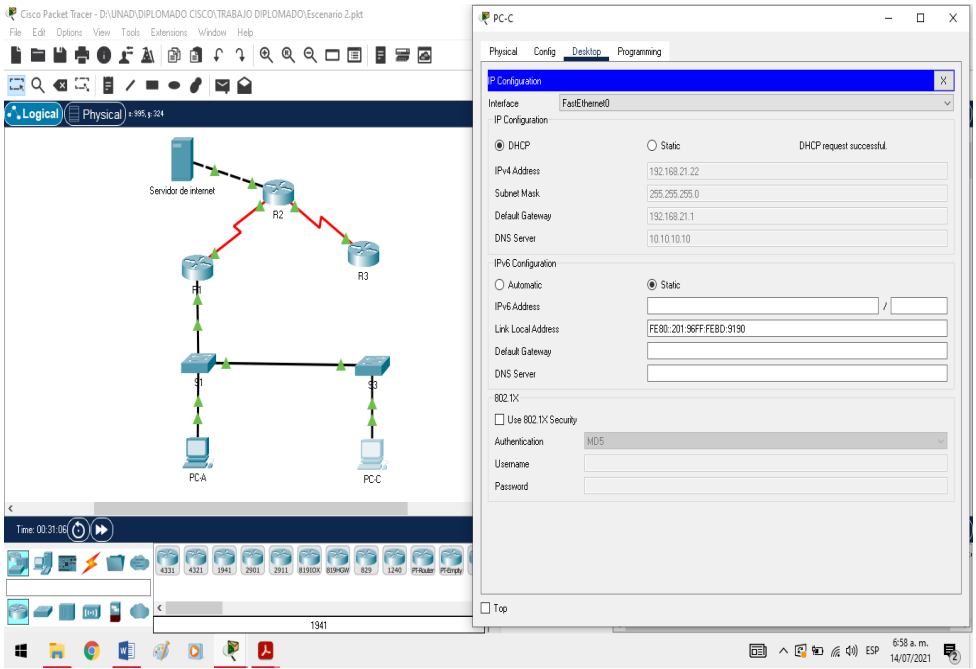
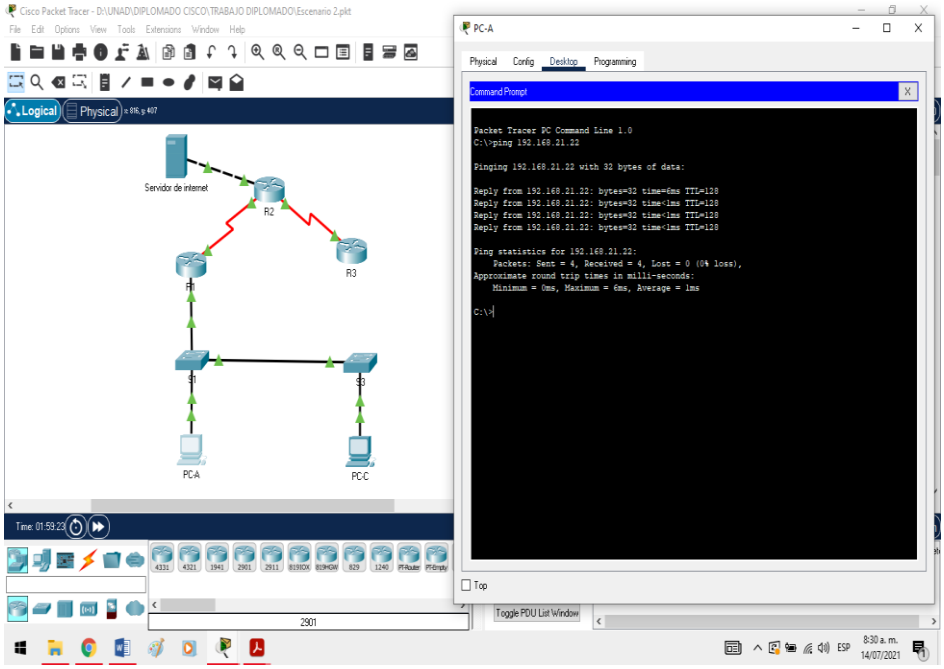


Figura 38. Ping PC-A a PC-C



PARTE 6

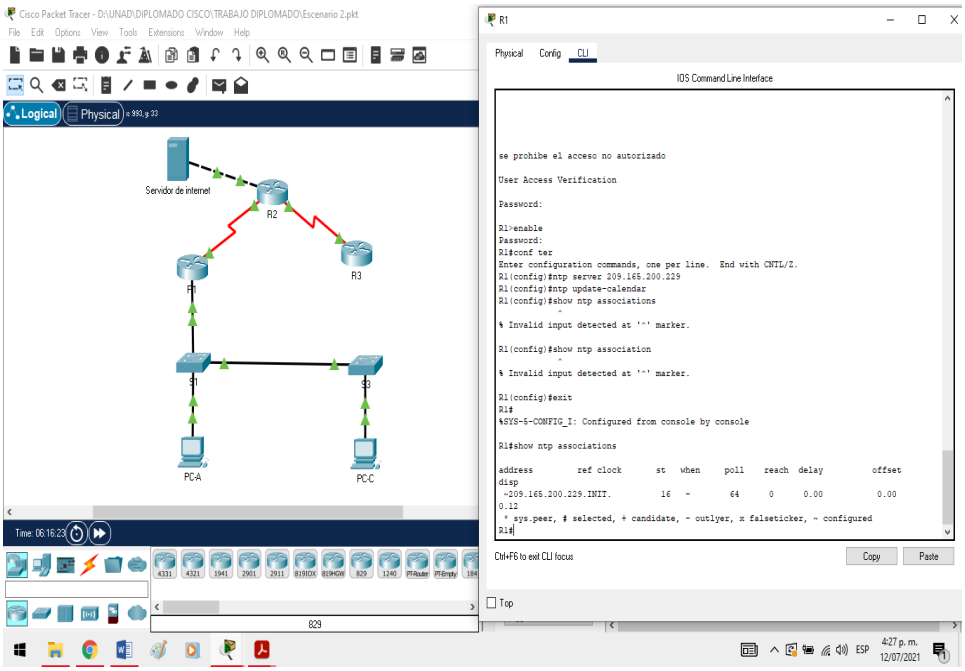
CONFIGURAR NAT

TABLA 31. DE CONFIGURACION NAT

ELEMENTO O TAREA A CONFIGURAR	ESPECIFICACION
Ajuste la fecha y hora en R2	5 DE MARZO DE 2016, 9 a.m. R2#clock set 09:00:00 05 march 2016
Configure R2 como maestro NTP	nivel de estrato: 5 R2(config)#ntp master 5
Configure R1 como un cliente NTP	servidor: R2 R1(config)#ntp server 209.165.200.229
Configure R1 para actualizaciones de calendario periódicas con hora NTP	R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1	R1# show ntp associations

Figura 39. configuración NAT



PARTE 7

CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

PASO 1: RESTRINGIR EL ACCESO A LAS LINEAS VTY EN EL R2

TABLA 32. RESTRICCIÓN DE ACCESOS LÍNEAS VTY R2

ELEMENTO O TAREA A CONFIGURAR	ESPECIFICACION
Configurar una lista de acceso con nombre para permitir que solo R1	Nombre de la ACL: ADMIN-MGT

establezca una conexión Telnet con R2	R2(config)#ip Access-list standard ADMIN-MGT
aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit R2(config)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R2#telnet 172.16.1.2

PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTAR LO SIGUIENTE

TABLA 33. COMANDOS DE MUESTREO DE ACL Y NAT

DESCRIPCION DEL COMANDO	ENTRADA DEL ESTUDIANTE (COMANDO)
Mostar las coincidencias recibidas por una lista de acceso desde la ultima vez que se reestableció.	Show Access list
Reestablecer los contadores de una lista de acceso	Clear Access-list counters
¿Qué comando se usa para mostrar que ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con que comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat statistics

Figura 40. interfaces R2

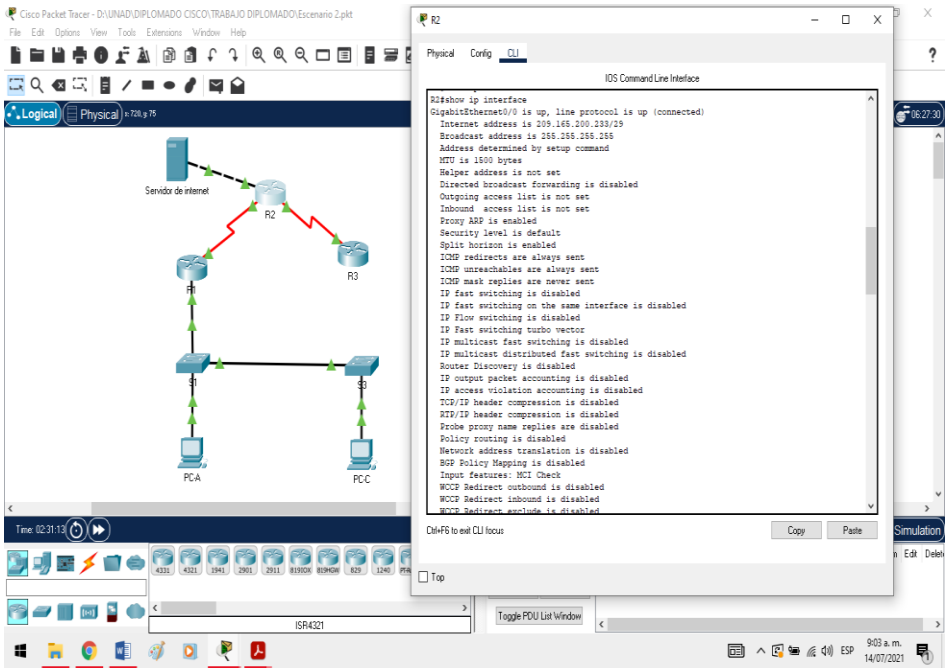
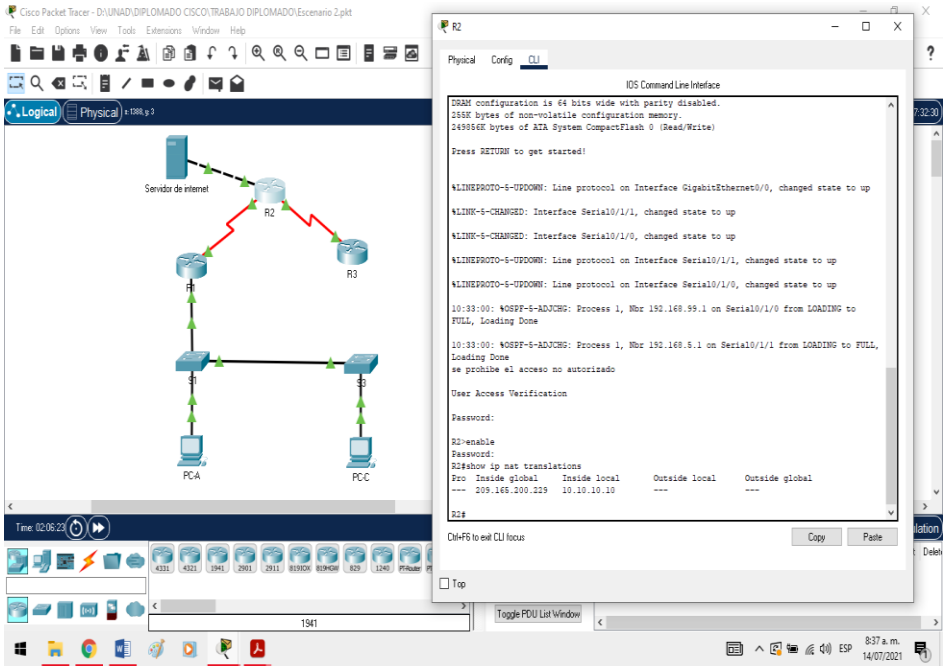


Figura 41. traducciones NAT R2



CONCLUSIONES

Con esta prueba de habilidades en este escenario llevamos a cabo la realización del ejercicio mediante las herramientas de simulación y con el material de apoyo documental por parte de cisco y profesional de nuestros tutores de la unad, se configuro una red aplicando los protocolos y los enrutamientos entre la VLAN y brindando protocolos de seguridad que permiten dar confianza a la red que solo personal idóneo realice los ajustes con usurario y password en los dispositivos de los dos escenarios

En los escenarios los dispositivos funcionan correctamente de los switchs y los router y los puertos habilitados permitiendo que los datos no se pierden y lleguen a su destino y se pudo evidenciar por el comando ping la conectividad y la asignación de las dirección y protocolos tanto como para la conexión de internet de los dispositivos, como para los demás equipos este se realizaron en los dos escenarios propuestos evidenciando que no hay perdida de datos y la completa conexión entre los mismos.

En la administración de la red del escenario 1 nos permitió nombre las distintas VLAN deshabilitar los puertos que no se utilizan, aviso de acceso no autorizado esto permite confianza en una red si se implementara en una red corporativa y con más dispositivos brindando la seguridad en la información que se maneje en la red, en el escenario 2 se configuro los dispositivos con direcciones dinámicas y estáticas NAT, con direcciones IPv4 para las comunicaciones mejorando el funcionamiento de la red por que busca utilizar menos recursos de los equipos en la creación de ACL.

BIBLIOGRAFIA

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2014) Entendiendo plantillas switch CISCO (sdm Templates CISCO) CDM sistemas

https://cmdsistemas.wordpress.com/2014/03/11/plantillas-switch-cisco-sdm-templates-cisco/

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5