SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JOSE LEONARDO GARCIA MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
FACATATIVA
NOVIEMBRE 2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

JOSE LEONARDO GARCIA MARTINEZ

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR:

ING.DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
FACATATIVA
NOVIEMBRE 2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Facatativá, 20 de noviembre de 2020

AGRADECIMIENTOS

Este trabajo se llevó a cabo de la mejor manera y quiero agradecer a la tutores Paulita Flor y Diego Edinson Ramirez por la información suministrada y el apoyo brindado en el desarrollo de este trabajo y a cada uno de los compañeros con los que se interactuó para poder resolver los inconvenientes e inquietudes presentadas, las cuales fueron de gran ayuda y a jehová dios por las oportunidades que me ha brindado día a día para poder culminar las metas profesionales propuestas.

TABLA DE CONTENIDO

AGRADECIMIENTOS 4

LISTA DE TABLAS 7

LISTA DE FIGURAS 8

GLOSARIO 9

RESUMEN 10

ABSTRACT 11

INTRODUCCIÓN 12

Desarrollo 13

1. Escenario 1 13

1.1 Parte 1 inicializar, configurar los dispositivos 14
1.1.1 Paso 1 inicializar y cargar el router y los switch 14
1.2 Paso 2 configurar router 1 15
1.3 Paso 3: configure s1 y s2. 19
1.3.1 Paso 3: configure s1 19
1.3.2 Paso 3: configure s2 21

1.4 Parte 2: Configuración de red vlan, Trunking, EtherChannel 22
1.4.1 Paso 4: configurar s1 22
1.4.2 Paso 5: configure el s2. 25

1.5 Parte 2: configurar soporte de host 28
1.5.1 Paso 6: configure r1 28
1.6 Paso 7: configurar los servidores 29

1.7 Parte 3 probar y verificar la conectividad de extremo a extremo 31

1.7.1 Paso 8: verificación de conectividad de pc-a a dispositivos 31

1.7.2 Paso 9: verificación de conectividad de pc-b a dispositivos 34

2.1 Parte 1 inicializar, configurar los dispositivos 38
2.1.1 Paso 1 inicializar y cargar el router y los switch 38

2.2 Parte 2 configuraciones básicas de los dispositivos 39
2.2.1 Paso 1 configurar la computadora de internet 39
2.2.2 Paso 2 configurar router 1 39
2.2.3 Paso 3 configurar router 2 41
2.2.4 Paso 4 configurar router 3 43
2.2.5 Paso 5 configurar swicth 1 44
2.2.6 Paso 6 configurar switch 3 45
2.2.7 Paso 7 verificar conectividad en la red 47
2.3 Parte 3 configuraciones de seguridad en los switch y routers en las vlan 49
2.3.1 Paso 1 configurar s1 49
2.3.2 Paso 2 configurar s3 50
2.3.3 Paso 3 configurar r1 51
2.3.4 Paso 4 verificación de conectividad entre los dispositivos 53
2.4 parte 4 configuraciones de protocolo routing dinámico OSPF 56
2.4.1 paso 1 configurar OSPF en r1 56
2.4.2 Paso 2 configurar OSPF en r2 57
2.4.3 Paso 3 configurar ospfv3 en r3 58
2.4.4 Paso 4 verificación información OSPF 59
2.5 Parte 5 implementación de DHCP y NAT para ipv4 59
2.5.1 Paso 1 configurar r1 en vlan 21,23 59
2.5.2 Paso 2 configurar NAT estática y dinámica en r2 61
2.5.3 Paso 3 verificación del protocolo DHCP y la NAT 62
2.6 Parte 6 configuración de NTP 64
2.7 Parte 7 configuración y validación de lista de acceso ACL 65
2.7.1 Paso 1 restringir acceso a vty en r2 65
2.7.2 Paso 2 verificar el comando CLI para mostrar información 66

CONCLUSIONES 68

BIBLIOGRAFIA 69

ANEXOS 70

LISTA DE TABLAS

Tabla 1. Inicializar dispositivos 15
Tabla 2. Configurar R1 16
Tabla 3. Configurar Switch 1 20
Tabla 4. Configurar Switch 2 21
Tabla 5. Tares de Configuracion Del Switch 1 23
Tabla 6. Tares de Configuracion Del Switch 2 26
Tabla 7. Tares de Configuracion Del Router 1 28
Tabla 8. Configuracion de PC-A 30
Tabla 9. Configuracion de PC-B 31
Tabla 10. Verificación de conectividad de PC-A a dispositivos 31
Tabla 11. Verificación de conectividad de PC-B a dispositivos 34
Tabla 12. Inicializar dispositivos escenario 2 38
Tabla 13. Configurar la computadora de internet 39
Tabla 14. Configurar R1 40
Tabla 15. Configurar R2 41
Tabla 16. Configurar R3 43
Tabla 17. Configurar S1 45
Tabla 18. Configurar S3 46
Tabla 19. Verificación de conectividad entre dispositivos 47
Tabla 20. Tareas De Configuracion Del Switch 1 50
Tabla 21. Tareas De Configuracion Del Switch 3 51
Tabla 22 Tareas De Configuracion Del Router 1 52
Tabla 23. Verificación de conectividad entre los switches y el R1 53
Tabla 24. Configurar OSPF en el R1 56
Tabla 25. Configurar OSPF en el R2 57
Tabla 26. Configurar OSPF en el R3 58
Tabla 27. Verificar Informacion De OSPF 59
Tabla 28. Configurar R1 Como DHCP Para VLAN 21 y 23 60
Tabla 29. Configurar NAT En R2 61
Tabla 30. Verificación De Protocolo DHCP Y NAT 62
Tabla 31. Configurar NTP 64
Tabla 32. Configurar Las Listas (ACL) 65
Tabla 33. Comandos CLI 66

LISTA DE FIGURAS

Figura 1. Escenario 1 13
Figura 2. Simulación de escenario 1 13
Figura 3. configurar router 1 16
Figura 4. Configurar Switch 1 19
Figura 5. Configurar Switch 2 26
Figura 6. Configuracion de PC-A 29
Figura 7. Configuracion de PC-B 30
Figura 8. Ping desde PC-A Hacia R1 - 10.19.8.1 32
Figura 9. Ping desde PC-A Hacia R1 - 2001:db8:acad:a: :1 33
Figura 10. Ping desde PC-A Hacia R1 - 10.19.8.65 33
Figura 11. Ping desde PC-A Hacia R1 - 2001:db8:acad:b: :1 34
Figura 12. Ping desde PC-B Hacia R1 – 209.165.201.1 35
Figura 13. Ping desde PC-B Hacia S1 – 10.19.8.98 35
Figura 14. Ping desde PC-B Hacia S1 – 2001:db8:acad:c: :98 36
Figura 15. Ping desde PC-B Hacia S2 – 10.19.8.99 36
Figura 16. Escenario 2 37
Figura 17. Simulación de escenario 2 37
Figura 18. configurar router 1 40
Figura 19. configurar router 3 43
Figura 20. configurar switch 3 46
Figura 21. Ping desde R1 Hacia R2, S0/0/0 47
Figura 22. Ping desde R2 Hacia R3, S0/0/1 47
Figura 23. Ping desde PC de Internet Hacia Gateway predeterminado 48
Figura 24. Configurar seguridad del Switch 1 49
Figura 25. configurar r1 subinterfaz 802.1Q 52
Figura 26. Ping desde S1 Hacia R1, dirección VLAN 99 53
Figura 27. Ping desde S3 Hacia R1, dirección VLAN 99 54
Figura 28. Ping desde S1 Hacia R1, dirección VLAN 21 54
Figura 29. Ping desde S3 Hacia R1, dirección VLAN 23 55
Figura 30. configurar OSPF en r1 56
Figura 31. configurar OSPF en r2 57
Figura 32. configurar r1 en vlan 21,23 60
Figura 33. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP 62
Figura 34. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP 63
Figura 35.Verificar que la PC-A pueda hacer ping a la PC-C 63
Figura 36. Verificar que la ACL funcione como se espera 65
Figura 37. Comando show access-list 67
Figura 38. Comando show ip interface 67

GLOSARIO

VLAN: (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

OSPF: (Open Shortest Path First) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).

NTP: (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

ETHERCHANNEL: es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast, Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

ACL: es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

IPV6: Es el Protocolo de Internet versión 6 o IPv6 (Internet Protocol version 6, en inglés) es una versión del Protocolo de Internet (IP). El Protocolo de Internet permite transmitir datos a través de una red a las direcciones IP (IPv4 o IPv6), que son las que identifican a los diferentes dispositivos conectados a Internet y permiten la comunicación entre ellos.

RESUMEN

En el presente trabajo se dará solución a dos escenarios planteados en la evaluación final de habilidades donde se pondrán en práctica los conocimientos adquiridos en el transcurso del diplomado. En el primer escenario se diseñó y configuro una red pequeña y sus dispositivos. Realizamos la configuración de 1 router,2 switch y 2 computadores que soporten la conectividad IPv4 y IPv6 donde se realizan las configuraciones de enrutamiento entre VLAN, DHCP, port-security y EtherChannel para que se puedan administrar de forma segura cada uno de los dispositivos de la red.

En el segundo escenario se diseñó y configuro una red pequeña y sus dispositivos. Realizamos la configuración de los 3 router,2 switch y 2 computadores y un servidor que soporten la conectividad IPv4 y IPv6 para los host. Los switches y los routers se deben gestionar de forma segura y debemos configurar el enrutamiento en las VLAN, usando el protocolo de enrutamiento OSPF y la configuración de hosts dinámicos DHCP y la traducción de direcciones de red dinámicas y estáticas NAT, también configuramos y verificamos las lista de control ACL y el protocolo de tiempo de red NTP y se realizan las respectivas verificaciones mediante los comando de CLI.

Palabras Clave: VLAN, DHCP, OSPF, NTP, EtherChannel, ACL.

ABSTRACT

This work will solve two scenarios raised in the final skills assessment where the knowledge acquired during the course will be put into practice. In the first scenario we must design and configure a small network and its devices. We proceed with the configuration of 1 router, 2 switches and 2 computers that support IPv4 and IPv6 connectivity where the routing configurations between VLAN, DHCP, port-security and EtherChannel are made so that each of the devices can be managed safely of the network. In the second scenario we must design and configure a small network and its devices. We proceed with the configuration of the 3 routers, 2 switches and 2 computers and a server that support IPv4 and IPv6 connectivity for the hosts. The switches and routers must be managed securely and we must configure the routing in the VLANs, using the OSPF routing protocol and the DHCP dynamic host configuration and the dynamic and static network address translation NAT, we also configure and verify the ACL checklist and NTP network time protocol and the respective checks are performed using the CLI commands.

Keywords: VLAN, DHCP, OSPF, NTP, EtherChannel, ACL).

INTRODUCCIÓN

En el desarrollo de este documento aplicaremos los conceptos adquiridos durante el diplomado de profundización CISCO CCNA dando solución a los escenarios propuestos en la prueba de habilidades, trabajando las configuraciones básicas y direccionamiento ipv4 y ipv6, protocolos y enrutamientos de los diferentes dispositivos para redes LAN/WAN.

El método de trabajo planteado para el desarrollo de los dos escenarios es el diseño de redes, seguridad, direccionamiento y configuraciones iniciales mediante el uso de comandos en cada uno de los dispositivos como lo son equipos, switches y routers para la combinación de cada uno de los protocolos de administración de redes en el IOS manejando comandos show y realizando tablas y figuras del paso a paso de las configuraciones de cada uno de los escenarios y validando configuración y funcionamiento de la red mediante comandos ping verificando la conexión correcta entre cada uno de los dispositivos mediante el software de aprendizaje Packet Tracer que nos permite realizar simulaciones lógicas y físicas de redes y configurar dispositivos, crear redes múltiples aplicando cada uno de los protocolos de redes como los son DHCP, (NAT), OSPF, NTP y ACL.

Desarrollo

1. Escenario 1

Figura 1. Escenario 1

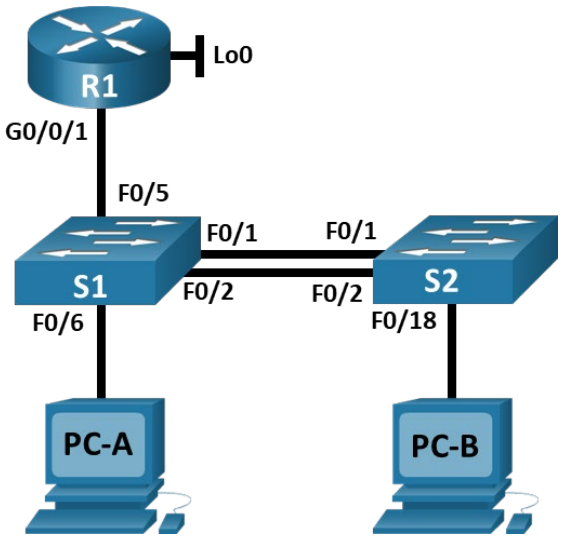
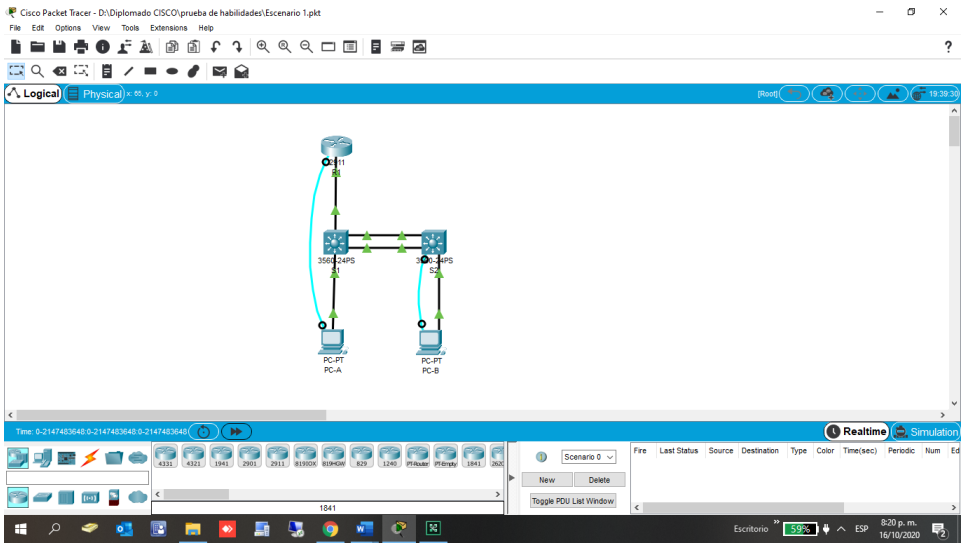


Figura 2. Simulación de escenario 1



Fuente: Autor

En el primer escenario debemos configurar una red pequeña y sus dispositivos. Procedemos con la configuración de 1 router,2 switch y 2 computadores que soporten la conectividad IPv4 como IPv6 para los host soportados. El switch y el routers se deben gestionar de forma segura. Por otro lado, debemos configura el enrutamiento en VLAN, DHCP, port-security Y EtherChannel.

1.1 Parte 1 inicializar, configurar los dispositivos

1.1.1 Paso 1 inicializar y cargar el router y los switch

Como primer paso para inicializar los dispositivos debemos borrar o eliminar las configuraciones de inicio para validar que estos no cuenten con alguna configuración más adelante no nos permita avanzar con cada uno de los pasos y nos genere errores en la configuración, al momento de cargar cada uno de los dispositivos. Para ello ejecutamos el comando erase startup-config para inicializar el router y los dos switch el cual sirve para eliminar la configuración de inicio predeterminada en la memoria NVRAM, también ejecutamos el comando Reload ya que este también se encarga de borrar la configuración de inicio para proceder con la carga de los dispositivos.

Debemos tener en cuenta la eliminación de los datos con el comando vlan.dat en memoria flash. Luego para proceder con la configuración de la plantilla SDM ejecutamos el comando sdm prefer dual-ipv4-and-ipv6 default para que permita IPv6 y se vuelva a cargar los switch nuevamente.

Tabla 1. Inicializar dispositivos

Instrucción de Configuracion	Configuracion
Desde el PC-A ingresamos al router y realizamos las configuraciones	Router>en Router#erase startup-config Router# reload
Inicializamos el switch S1	Switch>en Switch# erase startup-config Switch# delete vlan.dat Switch# reload
Inicializamos el switch S1	Switch>en Switch# erase startup-config Switch# delete vlan.dat Switch# reload
Volver a cargar el switch y configuramos la plantilla SDM.	Switch>enable Switch# show sdm prefer
Cargamos la plantilla sdm prefer en el switch 2 para que soporte IPv6.	Switch>configure terminal Switch# sdm prefer dual-ipv4-and-ipv6 default Switch# end Switch# reload
Procedemos con la configuración del switch 1 para que también soporte IPv6	Switch>configure terminal Switch# sdm prefer dual-ipv4-and-ipv6 default Switch# end Switch# reload

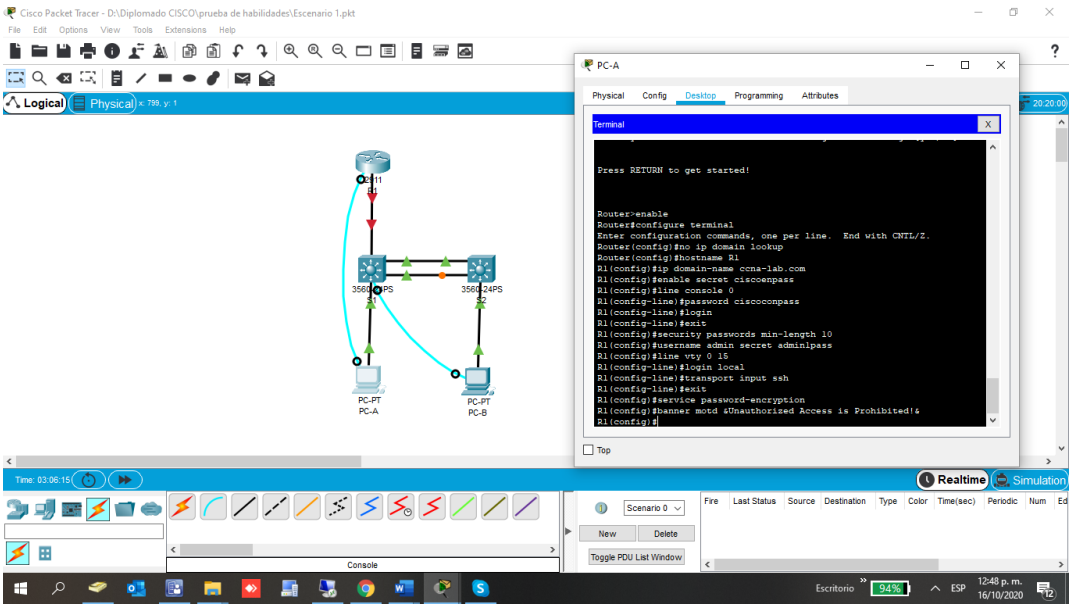
1.2 Paso 2 configurar router 1

Las configuraciones que realizamos en el Router son las siguientes:

En primer lugar, apagamos o desactivamos la búsqueda de DNS ya que si no lo hacemos se presentarán demoras y bloqueos al ingresar comandos de configuración si no contamos con servidor DNS. Por otro lado, para poder diferenciar nuestro router asignamos nombre y nombre del dominio, es importante asignar contraseña cifrada en modo EXEC y al puerto de consola

también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente ya que esto sería un foco de inseguridad para nuestro dispositivo. Algo importante en la configuración es generar un usuario y clave en la base de datos local y configurar el inicio de sesión en las líneas VTY para poder acceder a nuestro dispositivo a través de Telnet solo aceptando SSH y habilitamos el router ipv6 y cada una de las interfaces y generamos una clave de cifrado RSA para una mayor seguridad.

Figura 3. configurar router 1



Fuente: Autor

Tabla 2. Configurar R1

Tarea de configuración	Especificación de configuración
Deshabilitamos la búsqueda DNS	Router>enable Router>configure terminal Router (config)#no ip domain lookup
Asignamos nombre del router	Router (config)# hostname R1
Asignamos dominio	R1(config)#ip domain-name ccna-lab.com
Generamos password secreta en modo EXEC	R1(config)#enable secret ciscoenpass

Generamos password de acceso a la consola	R1(config)#line console 0 R1(config-line)# password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas 10 caracteres	R1(config)#security passwords min-length 10
Creamos un usuario y password en la base de datos local.	R1(config)#username admin secret admin1pass
Configuráramos el inicio en las líneas VTY	R1(config)#line vty 0 15 R1(config-line)#login local
Configuráramos VTY solo para SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las password de texto.	R1(config)#service password-encryption
Configuramos un MOTD Banner	R1(config)# banner motd &Unauthorized Access is Prohibited!&
Habilitar IPv6 en el router 1	R1(config)#ipv6 unicast-routing

Configurar la interfaz y subinterfaces en nuestro router asignado una descripción y establecer una dirección ipv4 y una dirección local ipv6 y proceder con la activación de la interfaz .	R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config)#int g0/0/1.3 R1(config-subif)#encapsulation dotlq 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dotlq 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config)#int g0/0/1.6 R1(config-subif)#encapsulation dotlq 6 R1(config-subif)#description Native R1(config)#int g0/0/1 R1(config-subif)#shutdown
Configurar el Loopback 0 interface	R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description cloud R1(config-if)#exit

Generar un password de cifrado RSA de 1024 bits	R1(config)#crypto key generate rsa general-key modulus 1024 R1(config)#exit

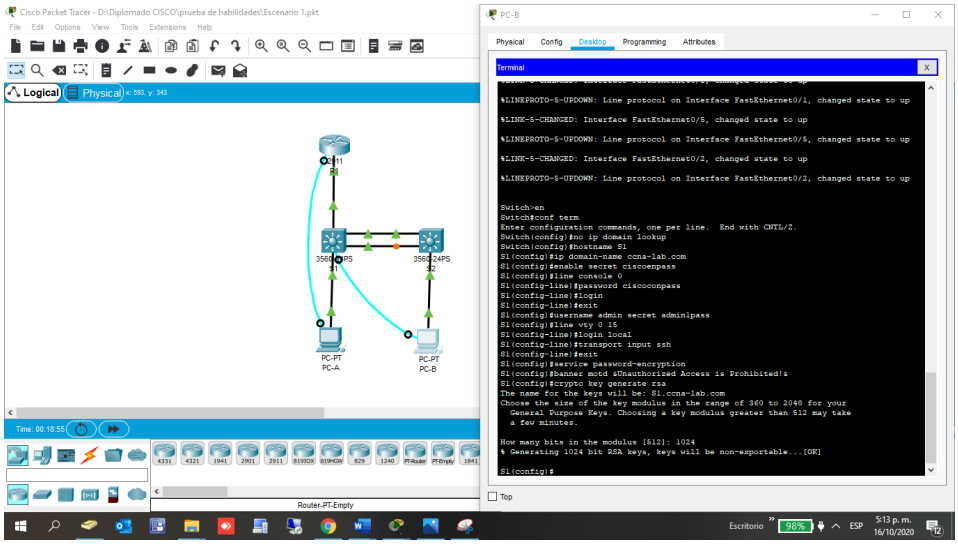
1.3 Paso 3: configure s1 y s2.

1.3.1 Paso 3: configure s1

Las configuraciones que realizamos en el switch 1 son las siguientes:

En primer lugar, apagamos o desactivamos la búsqueda de DNS. Por otro lado, para poder diferenciar nuestro switch asignamos nombre y nombre del dominio, es importante asignar contraseña cifrada en modo EXEC y al puerto de consola también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente a nuestro switch configuramos un MOTD Banner. También configuramos la interfaz de administración (SVI) como lo sabemos esta es una interfaz virtual, no asociada a ningún puerto físico de nuestro switch por ellos es importante la configuración del Gateway predeterminado.

Figura 4. Configurar Switch 1



Fuente: Autor

Tabla 3. Configurar Switch 1

Tarea	Especificación
Deshabilitamos la búsqueda DNS	Switch>en Switch#conf term Switch(config)#no ip domain lookup
Asignamos nombre a switch S1	Switch(config)#hostname S1
Asignamos dominio a switch S1	S1(config)#ip domain-name ccna-lab.com
Generamos password secreta en modo EXEC	S1(config)#enable secret ciscoenpass
Generamos password de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Creamos un usuario y password en la base de datos local.	S1(config)#username admin secret admin1pass
Configuráramos el inicio en las líneas VTY	S1(config)#line vty 0 15 S1(config-line)#login local
Configuráramos VTY solo para SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las password de texto.	S1(config)#service password-encryption
Configuramos un MOTD Banner	S1(config)#banner motd &Unauthorized Access is Prohibited!&
Generar un password de cifrado RSA de 1024 bits	S1(config)#crypto key generate rsa general-key modulus 1024 S1(config)#exit

Configuramos la interfaz (SVI)	S1(config)#int vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Management interface S1(config-if)#no shutdown S1(config-if)#exit
Configuramos el Gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

1.3.2 Paso 3: configure s2

Las configuraciones que realizamos en el switch 2 son las siguientes:

En primer lugar, apagamos o desactivamos la búsqueda de DNS. Por otro lado, para poder diferenciar nuestro switch asignamos nombre y nombre del dominio, es importante asignar contraseña cifrada en modo EXEC y al puerto de consola también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente a nuestro switch configuramos un MOTD Banner. También configuramos la interfaz de administración (SVI) como lo sabemos esta es una interfaz virtual, no asociada a ningún puerto físico de nuestro switch por ellos es importante la configuración del Gateway predeterminado.

Tabla 4. Configurar Switch 2

Tarea	Especificación
Deshabilitamos la búsqueda DNS	Switch>en Switch#conf term Switch(config)#no ip domain lookup
Asignamos nombre a switch S2	Switch(config)#hostname S2
Asignamos dominio a switch S2	S2(config)#ip domain-name ccna-lab.com

Generamos password secreta en modo EXEC	S2(config)#enable secret ciscoenpass
Generamos password de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Creamos un usuario y password en la base de datos local.	S2(config)#username admin secret admin1pass
Configuráramos el inicio en las líneas VTY	S2(config)#line vty 0 15 S2(config-line)#login local
Configuráramos VTY solo para SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las password de texto.	S2(config)#service password-encryption
Configuramos un MOTD Banner	S2(config)#banner motd &authorized Access is prohibited!&
Generar un password de cifrado RSA de 1024 bits	S2(config)#crypto key generate rsa general-key modulus 1024 S2(config)#exit
Configuramos la interfaz (SVI)	S2(config)#int vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Management interface S2(config-if)#no shutdown S2(config-if)#exit
Configuramos el Gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

1.4 Parte 2: Configuración de red vlan, Trunking, EtherChannel

1.4.1 Paso 4: configurar s1

Las configuraciones que realizamos en el switch 1 son las siguientes:

En primer lugar, realizamos la creación de las VLAN y creamos troncos que utilicen la VLAN 6 nativa y configuramos interfaces. Por otro lado, Creamos un grupo de puertos EtherChannel de la Capa 2 para algunas interfaces utilizando el comando #channel-group 1 mode active. Algo importante para resaltar en esta configuración es el uso del protocolo LACP para la negociación, el cual que permite agrupar varios puertos físicos para unificar un único canal lógico.

También configuramos el puerto de acceso de host y se configuramos la seguridad en los puertos de acceso a direcciones MAC y algo para tener en cuenta es que en toda configuración debemos proteger las interfaces no utilizadas y asignarlas a determinada VLAN, para ello ejecutamos el comando #switchport mode access para dejar en modo de acceso y asignamos una descripción y apagamos.

Tabla 5. Tares de Configuracion Del Switch 1

Tarea	Especificación
Creamos las diferentes VLAN	S1(config)#vlan 2 S1(config-vlan)#name bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit

Creamos los troncos que utilicen la VLAN 6 nativa en las Interfaces F0/1, F0/2 y F0/5	S1(config)#int f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)# S1(config-if)#int range f0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Creamos un grupo EtherChannel que use interfaces F0/1 y F0/2	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configuramos el puerto de host para VLAN 2 en la Interface F0/6	S1(config-if)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configuramos la seguridad del puerto en los en3 direcciones MAC	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3

Asignamos la VLAN 5 a todas las interfaces no utilizadas.	S1(config-if)#int range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not in use S1(config-if-range)#shutdown S1(config-if-range)#int range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not in use S1(config-if-range)#shutdown S1(config-if-range)#int range f0/1-2 S1(config-if-range)#no shutdown

1.4.2 Paso 5: configure el s2.

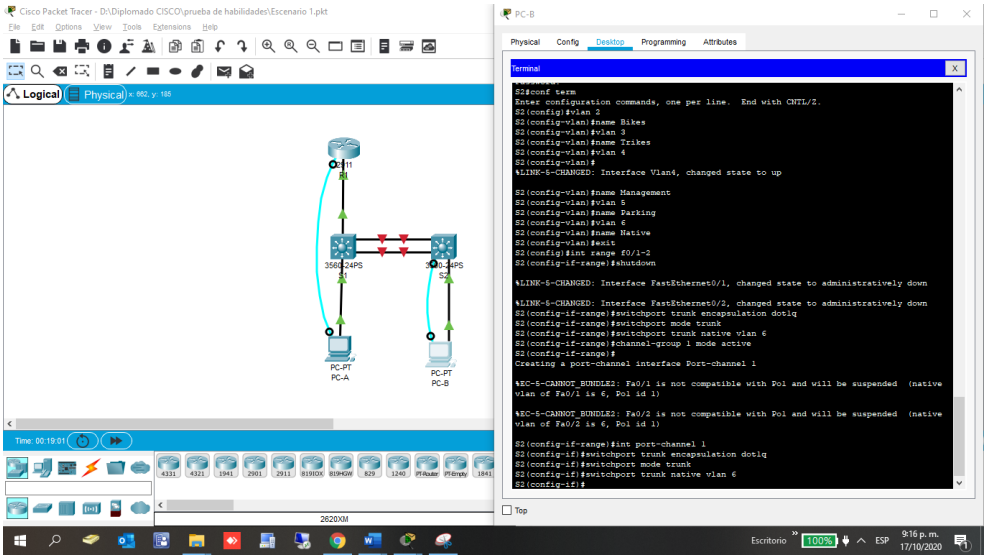
Las configuraciones que realizamos en el switch 2 son las siguientes:

En primer lugar, realizamos la creación de las VLAN y creamos troncos que utilicen la VLAN 6 nativa y configuramos interfaces. Por otro lado, Creamos un grupo de puertos EtherChannel de la Capa 2 para algunas interfaces utilizando el comando #channel-group 1 mode active. Algo importante para resaltar en esta configuración es el uso del protocolo LACP para la negociación, el cual que permite agrupar varios puertos físicos para unificar un único canal lógico.

También configuramos el puerto de acceso de host y se configuramos la seguridad en los puertos de acceso a direcciones MAC y algo para tener en cuenta es que en toda configuración debemos proteger las interfaces no utilizadas y asignarlas a determinada VLAN, para ello ejecutamos el comando

#switchport mode access para dejar en modo de acceso y asignamos una descripción y apagamos.

Figura 5. Configurar Switch 2



Fuente: Autor

Tabla 6. Tares de Configuracion Del Switch 2

Tarea	Especificación
Creamos las diferentes VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit

Creamos los troncos que utilicen la VLAN 6 nativa en las Interfaces F0/1, F0/2 y F0/5	S2(config)#int range f0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Creamos un grupo EtherChannel que use interfaces F0/1 y F0/2	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configuramos el puerto de host para VLAN 2 en la Interface F0/6	S2(config-if)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configuramos la seguridad del puerto en los en3 direcciones MAC	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3

Asignamos la VLAN 5 a todas las interfaces no utilizadas.	S2(config-if)#int range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in use S2(config-if-range)#shutdown S2(config-if-range)#int range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not in use S2(config-if-range)#shutdown S2(config-if-range)#int range f0/1-2 S2(config-if-range)#no shutdown

1.5 Parte 2: configurar soporte de host

1.5.1 Paso 6: configure r1

Las configuraciones en el router R1 DHCP para IPv4 para las VLAN indicadas y asignamos el nombre de dominio y puerta de enlace predeterminada

Tabla 7. Tares de Configuracion Del Router 1

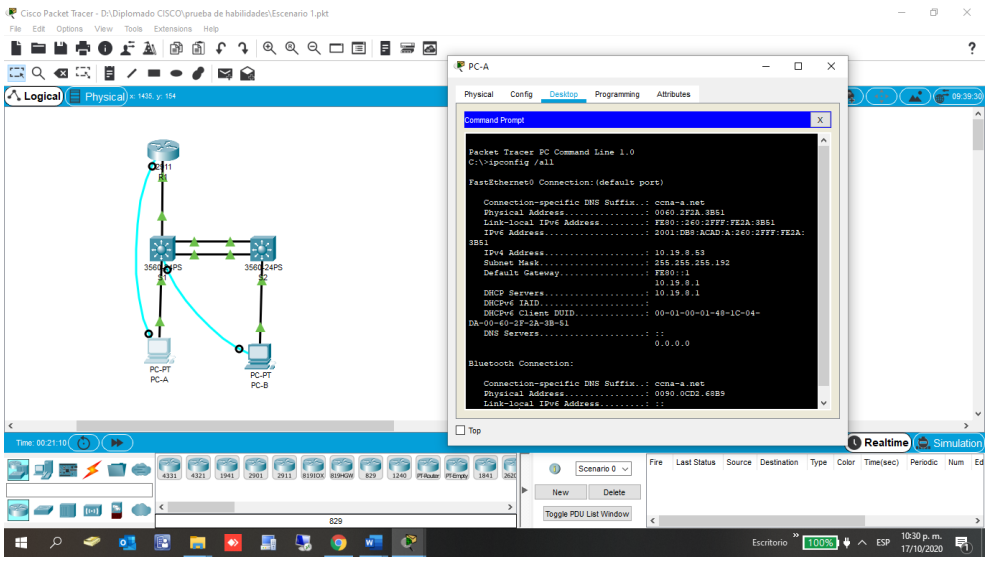
Tarea	Especificación
Configuramos rutas predeterminadas para IPv4, IPv6 que dirijan el tráfico a Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0

Configuráramos DHCP para IPv4 para la VLAN 2 y asignamos el nombre de dominio y puerta de enlace.	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configuráramos DHCP para IPv4 para VLAN 3 2 y asignamos el nombre de dominio y puerta de enlace.	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

1.6 Paso 7: configurar los servidores

Configuramos los equipos host PC-A y PC-B para que manejen DHCP para IPv4 y se les asigne las direcciones IPv6 GUA y Link Local. Después de configurar cada equipo, anotamos las configuraciones de red del host con el comando ipconfig /all como se muestra en la siguiente figura.

Figura 6. Configuracion de PC-A

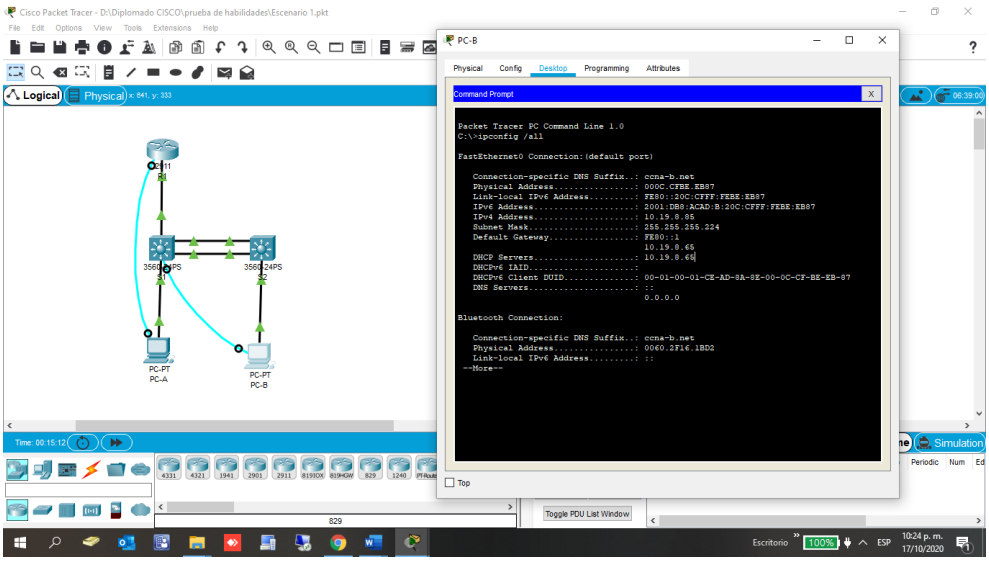


Fuente: Autor

Tabla 8. Configuracion de PC-A

PC-A Network Configuration	
Descripción	Connection-specific DNS Suffix..: ccna-a.net
Direc. Física	Physical Address.....: 0060.2F2A.3B51
Direc. IP	IPv4 Address.....: 10.19.8.53
Subnet Mask	Subnet Mask.....: 255.255.255.192
Gateway	10.19.8.1
Gateway IPv6	Default Gateway.....: FE80::1

Figura 7. Configuracion de PC-B



Fuente: Autor

Tabla 9. Configuracion de PC-B

Configuración de red de PC-B	
Descripción	Connection-specific DNS Suffix..: ccna-b.net
Dirección física	Physical Address.....: 000C.CFBE.EB87
Dirección IP	IPv4 Address.....: 10.19.8.85
Máscara de subred	Subnet Mask.....: 255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	Default Gateway.....: FE80::1

1.7 Parte 3 probar y verificar la conectividad de extremo a extremo

1.7.1 Paso 8: verificación de conectividad de pc-a a dispositivos

Este es uno de los pasos más importantes ya que es donde validamos la configuraciones realizadas anterior entre en cada uno de nuestros dispositivos para ellos utilizamos nuestro comando de ping para validar la conectividad IPv4 e IPv6 entre todos los dispositivos de nuestra red. Algo positivo en la configuración de la red es que todos los ping entre los diferentes dispositivos respondieron satisfactoriamente para lograr un 100% de configuración total de la red.

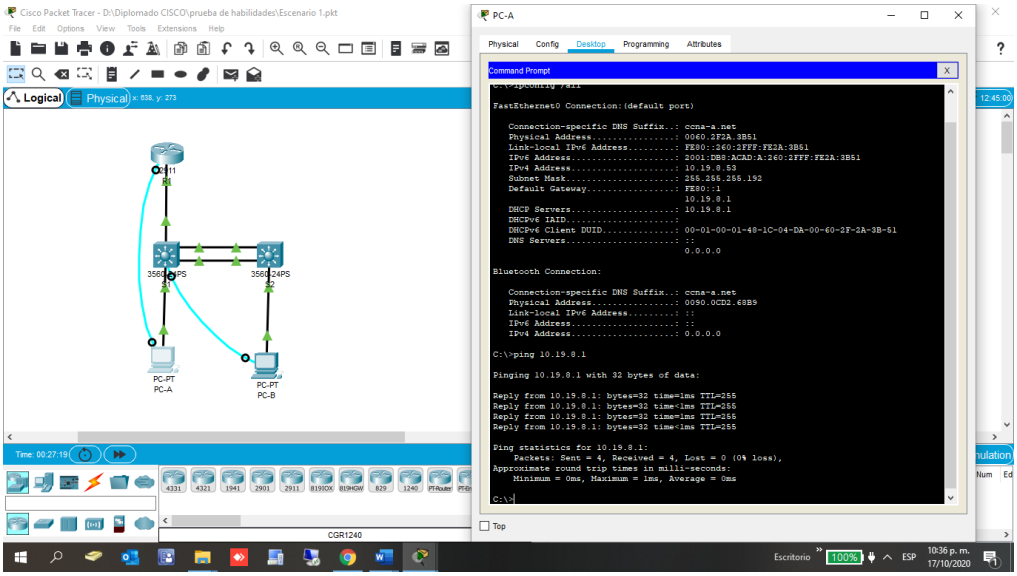
Tabla 10. Verificación de conectividad de PC-A a dispositivos

Desde	A	de Internet	Dirección IP	Ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Ok
		IPv6	2001:db8:acad:a: :1	Ok

	R1, G0/0/1.3	Dirección	10.19.8.65	Ok
		IPv6	2001:db8:acad:b: :1	Ok
	R1, G0/0/1.4	Dirección	10.19.8.97	Ok
		IPv6	2001:db8:acad:c: :1	Ok
	S1, VLAN 4	Dirección	10.19.8.98	Ok
		IPv6	2001:db8:acad:c: :98	Ok
	S2, VLAN 4	Dirección	10.19.8.99	Ok
		IPv6	2001:db8:acad:c: :99	Ok
	PC-B	Dirección	IP address will vary.	Ok
		IPv6	2001:db8:acad:b: :50	Ok
	R1 Bucle 0	Dirección	209.165.201.1	Ok
		IPv6	2001:db8:acad:209: :1	Ok

Se realiza el ping de verificación desde PC-A Hacia R1 - 10.19.8.1

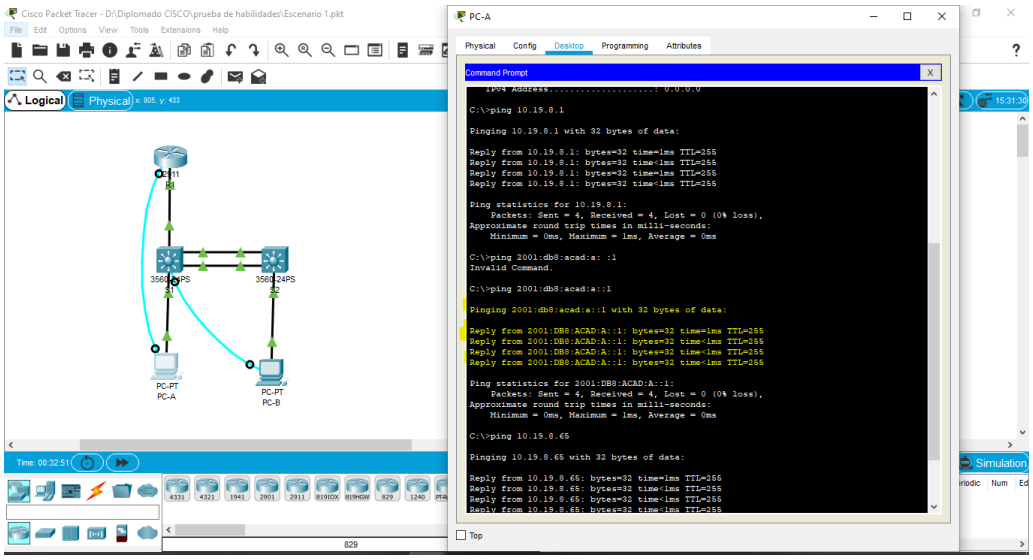
Figura 8. Ping desde PC-A Hacia R1 - 10.19.8.1



Fuente: Autor

Se realiza el ping de verificación desde PC-A Hacia R1 - 2001:db8:acad:a: :1

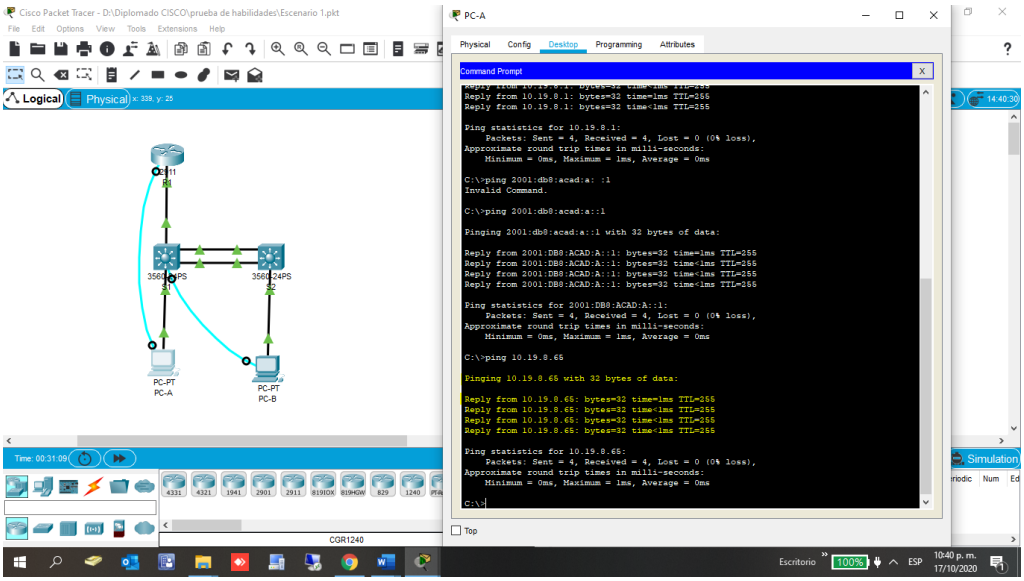
Figura 9. Ping desde PC-A Hacia R1 - 2001:db8:acad:a: :1



Fuente: Autor

Se realiza el ping de verificación desde PC-A A R1, G0/0/1. A la dirección IP 10.19.8.65.

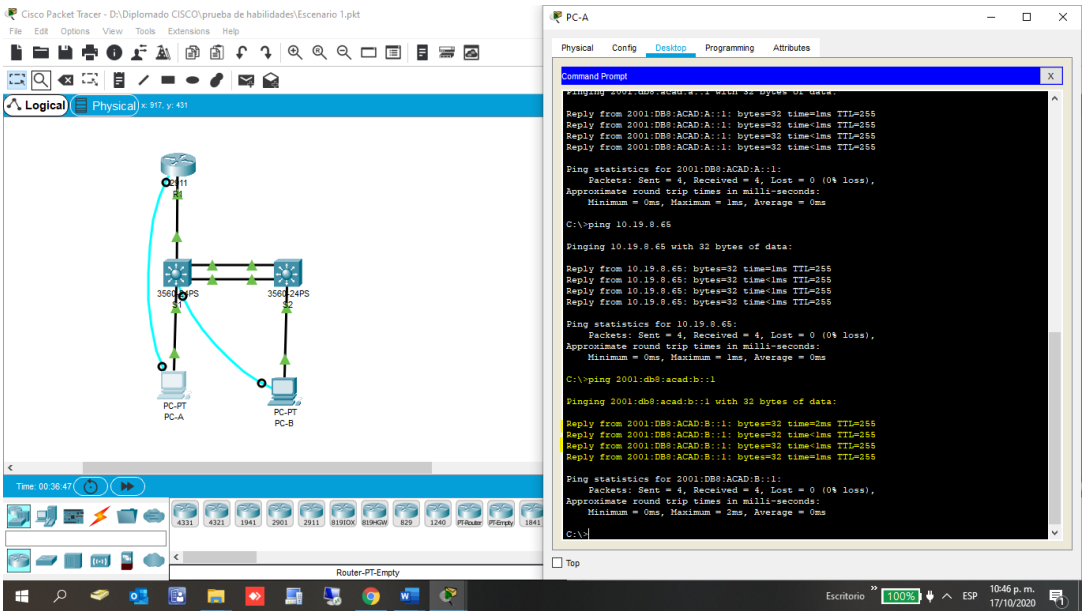
Figura 10. Ping desde PC-A Hacia R1 - 10.19.8.65



Fuente: Autor

Se realiza el ping de verificación desde PC-A Hacia R1 - 2001:db8:acad:b: :1

Figura 11. Ping desde PC-A Hacia R1 - 2001:db8:acad:b: :1



Fuente: Autor

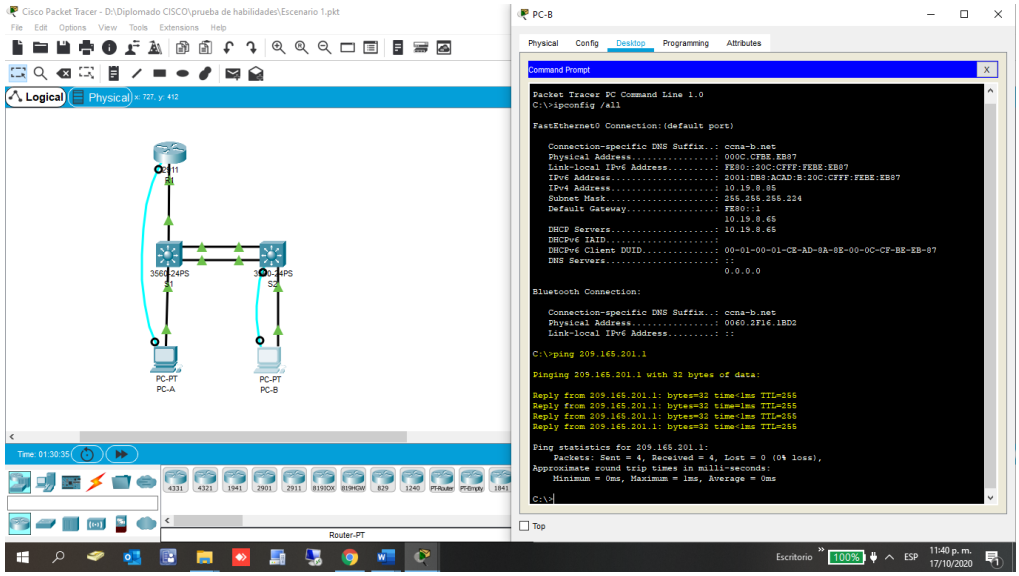
1.7.2 Paso 9: verificación de conectividad de pc-b a dispositivos

Tabla 11. Verificación de conectividad de PC-B a dispositivos

Desde	A	de Internet	Dirección IP	ping
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Ok
		IPv6	2001:db8:acad:209: :1	Ok
	R1, G0/0/1.2	Dirección	10.19.8.1	Ok
		IPv6	2001:db8:acad:a: :1	Ok
	R1, G0/0/1.3	Dirección	10.19.8.65	Ok
		IPv6	2001:db8:acad:b: :1	Ok
	R1, G0/0/1.4	Dirección	10.19.8.97	Ok
		IPv6	2001:db8:acad:c: :1	Ok
	S1, VLAN 4	Dirección	10.19.8.98	Ok
		IPv6	2001:db8:acad:c: :98	Ok
	S2, VLAN 4	Dirección	10.19.8.99	Ok
		IPv6	2001:db8:acad:c: :99	Ok

Se realiza el ping de verificación desde PC-B Hacia R1 – 209.165.201.1:1

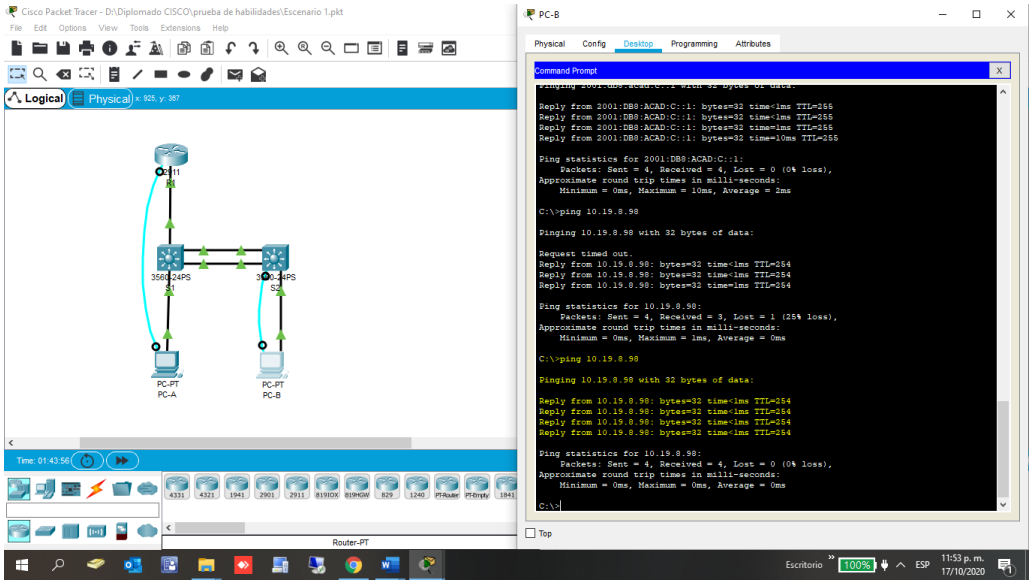
Figura 12. Ping desde PC-B Hacia R1 – 209.165.201.1



Fuente: Autor

Se realiza el ping de verificación desde PC-B Hacia S1 – 10.19.8.98

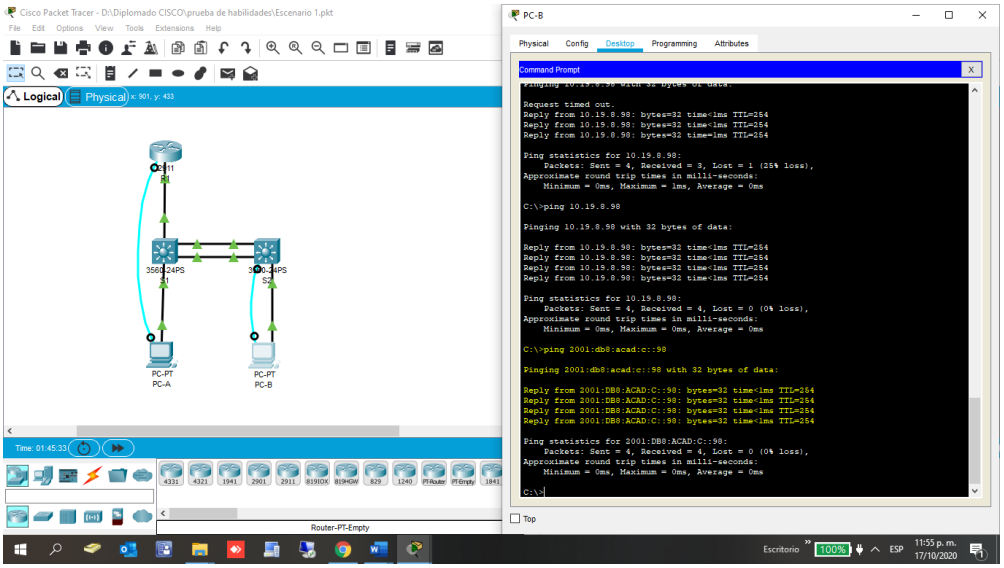
Figura 13. Ping desde PC-B Hacia S1 – 10.19.8.98



Fuente: Autor

Se realiza el ping de verificación desde PC-B Hacia S1 – 2001:db8:acad:c: :98

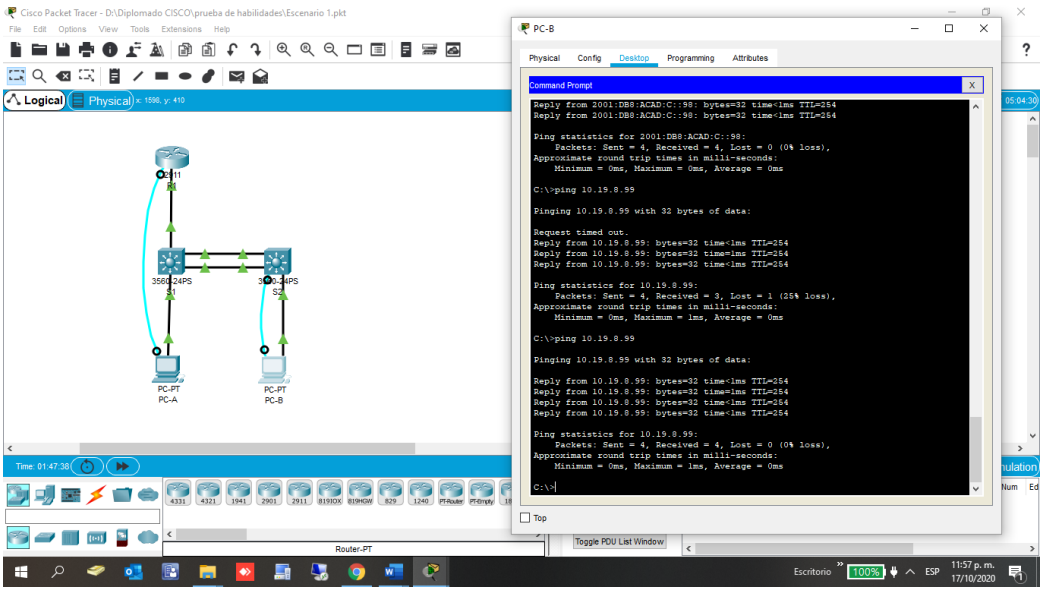
Figura 14. Ping desde PC-B Hacia S1 – 2001:db8:acad:c: :98



Fuente: Autor

Se realiza el ping de verificación desde PC-B Hacia S1 – 2001:db8:acad:c: :98

Figura 15. Ping desde PC-B Hacia S2 – 10.19.8.99



Fuente: Autor

Escenario 2

Figura 16. Escenario 2

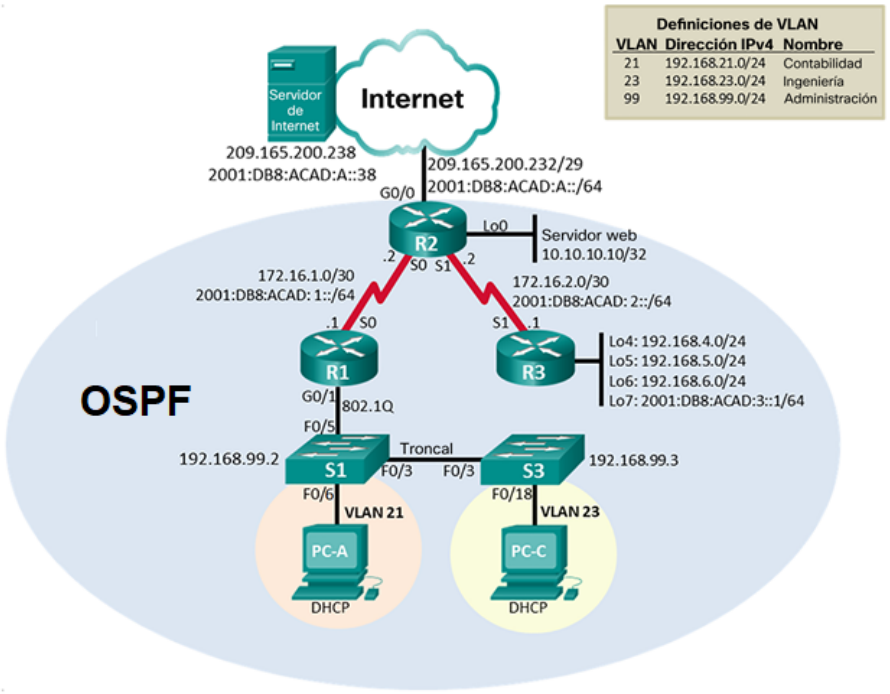
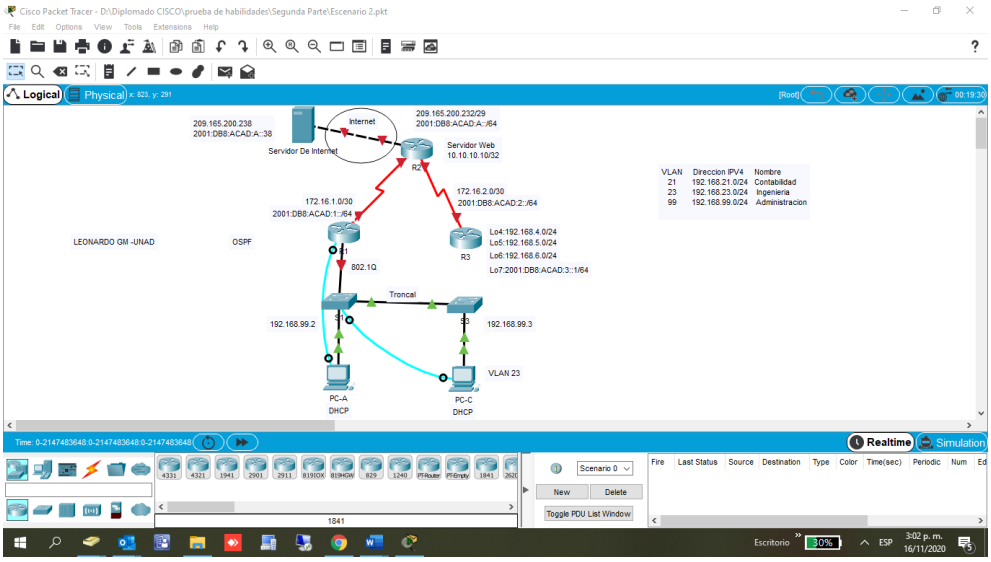


Figura 17. Simulación de escenario 2



Fuente: Autor

En el segundo escenario debemos configurar una red pequeña y sus dispositivos. Procedemos con la configuración de los 3 router,2 switch y 2 computadores y un servidor que soporten la conectividad IPv4 como IPv6 para los host soportados. Los switches y los routers se deben gestionar de forma segura. Por otro lado, debemos configurar el enrutamiento en VLAN, Protocolo dinámico OSPF,DHCP,NAT,ACL,NTP y se realizan las respetivas verificaciones mediante los comando de CLI.

2.1 Parte 1 inicializar, configurar los dispositivos

2.1.1 Paso 1 inicializar y cargar el router y los switch

Como primer paso para inicializar los dispositivos debemos borrar o eliminar las configuraciones de inicio para validar que estos no cuenten con alguna configuración más adelante no nos permita avanzar con cada uno de los pasos y nos genere errores en la configuración, al momento de cargar cada uno de los dispositivos. Para ello ejecutamos el comando erase startup-config para inicializar los router y los switch el cual sirve para eliminar la configuración de inicio predeterminada en la memoria NVRAM, también ejecutamos el comando Reload ya que este también se encarga de borrar la configuración de inicio para proceder con la carga de los dispositivos. Debemos tener en cuenta la eliminación de los datos con el comando vlan.dat en memoria flash.

Tabla 12. Inicializar dispositivos escenario 2

Tarea de configuración	Especificación de configuración
ingresamos al router y realizamos las configuraciones	Router>en Router#erase startup-config
cargamos los routers	Router# reload

Inicializamos los switch	Switch>en Switch# erase startup-config Switch# delete vlan.dat
Cargamos ambos switches	Switch# reload
Verificamos que la BD de VLAN no esté en la flash de ambos switches	Switch# show flash: Switch# show vlan brief

2.2 Parte 2 configuraciones básicas de los dispositivos

2.2.1 Paso 1 configurar la computadora de internet

Realizamos la configuración del servidor de Internet para obtener la respectiva información de las direcciones ip.

Tabla 13. Configurar la computadora de internet

Tarea de configuración	Especificación de configuración
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

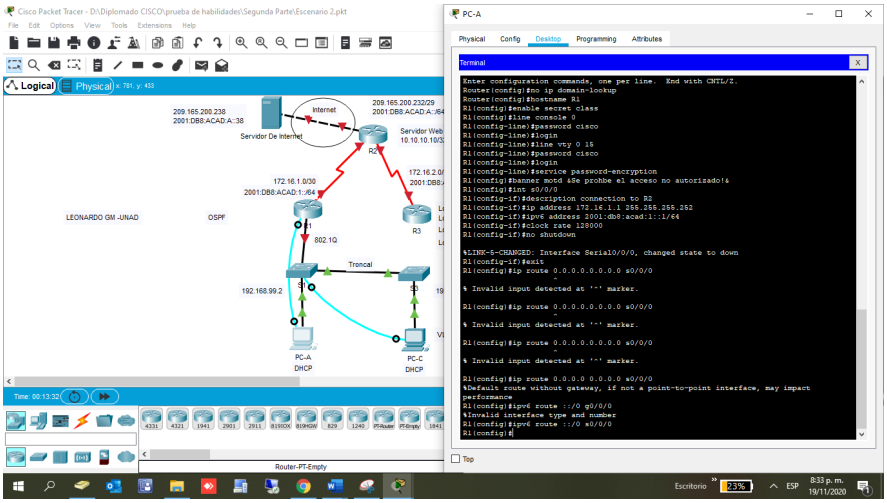
2.2.2 Paso 2 configurar router 1

Las configuraciones que realizamos en los 3 routers son las siguientes:

En primer lugar, apagamos o desactivamos la búsqueda de DNS ya que si no lo hacemos se presentarán demoras y bloqueos al ingresar comandos de configuración si no contamos con servidor DNS. Por otro lado, para poder diferenciar nuestro router asignamos nombre, es importante asignar contraseña cifrada en modo EXEC y al puerto de consola también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente ya que esto sería un foco de inseguridad para nuestro dispositivo.

Algo importante en la configuración es generar un usuario y clave en la base de datos local y configurar el inicio de sesión en las líneas VTY para poder acceder a nuestro dispositivo a través de Telnet y habilitamos el router ipv6 y cada una de las interfaces y configuramos las rutas predeterminadas de nuestros puertos seriales.

Figura 18. configurar router 1



Fuente: Autor

Tabla 14. Configurar R1

Tarea de configuración	Especificación de configuración
Deshabilitamos la búsqueda DNS	Router>enable Router#configure terminal Router (config)#no ip domain-lookup
Asignamos nombre del router	Router (config)#hostname R1
Generamos password secreta en modo EXEC	R1(config)#enable secret class
Generamos password de acceso a la consola	R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)#login

Generamos password y Configuráramos el inicio en las líneas VTY	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las password de texto.	R1(config-line)#service password-encryption
Configuramos un MOTD Banner	R1(config)# banner motd &Se prohíbe el acceso no autorizado!&
Configurar la interfaz y subinterfaces en nuestro router y asignar una descripción y establecer una dirección ipv4 y una dirección local ipv6 y establecer la frecuencia de reloj y proceder con la activación de la interfaz	R1(config)#int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Configurar las rutas predeterminadas ipv4 y ipv6 en los puertos seriales	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

2.2.3 Paso 3 configurar router 2

En primer lugar, para realizar la configuración del router 2 , apagamos o desactivamos la búsqueda DNS. Por otro lado, para poder diferenciar nuestro router asignamos nombre y configurar la seguridad en la consola con una contraseña y activamos la interfaz en nuestro router.

Tabla 15. Configurar R2

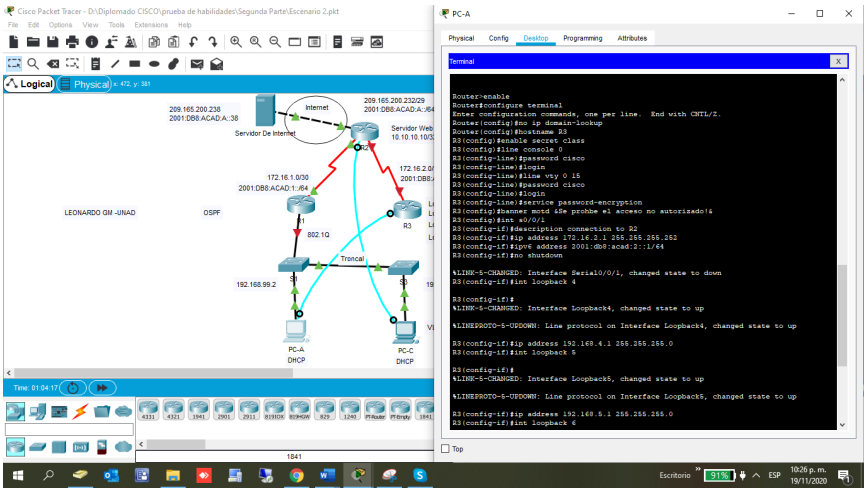
Tarea de configuración	Especificación de configuración
Deshabilitamos la búsqueda DNS	Router>enable Router#configure terminal Router (config)#no ip domain-lookup
Asignamos nombre del router	Router (config)#hostname R2
Generamos password secreta en modo EXEC	R2(config)#enable secret class
Generamos password de acceso a la consola	R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)#login

Generamos password y Configuráramos el inicio en las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las password de texto.	R2(config-line)#service password-encryption
Configuramos un MOTD Banner	R2(config)#banner motd &Se prohíbe el acceso no autorizado!&
Interfaz S0/0/0 Configurar la interfaz en nuestro router y asignar una descripción y establecer una dirección ipv4 y una dirección local ipv6 y proceder con la activación de la interfaz.	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1 Configurar la interfaz y subinterfaces en nuestro router y asignar una descripción y establecer una dirección ipv4 y una dirección local ipv6 y proceder con la activación de la interfaz	R2(config-if)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 Configurar la interfaz y subinterfaces en nuestro router y asignar una descripción y establecer una dirección ipv4 y una dirección local ipv6 y proceder con la activación de la interfaz.	R2(config-if)#int g0/0 R2(config-if)#description connection to internet R2(config-if)#ip address 209.165.200.233 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 Configurar la interfaz y asignar una descripción y establecer una dirección ipv4.	R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description web server R2(config-if)#exit
Configurar las rutas predeterminadas ipv4 y ipv6 en los puertos seriales	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

2.2.4 Paso 4 configurar router 3

Para realizar la configuración del router 3 , apagamos o desactivamos la búsqueda DNS y asignamos nombre y configuramos la seguridad en la consola con una contraseña y activamos la interfaz en nuestro router

Figura 19. configurar router 3



Fuente: Autor

Tabla 16. Configurar R3

Tarea de configuración	Especificación de configuración
Deshabilitamos la búsqueda DNS	Router>enable Router#configure terminal Router (config)#no ip domain-lookup
Asignamos nombre del router	Router (config)#hostname R3
Generamos password secreta en modo EXEC	R3(config)#enable secret class
Generamos password de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Generamos password y Configuráramos el inicio en las líneas VTY	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las password de texto.	R3(config-line)#service password-encryption

Configuramos un MOTD Banner	R3(config)#banner motd &Se prohíbe el acceso no autorizado!&
Interfaz S0/0/1 Configurar la interfaz y subinterfaces en nuestro router y asignar una descripción y establecer una dirección ipv4 y una dirección local ipv6 y proceder con la activación de la interfaz.	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4 Establecer una dirección ipv4.	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establecer una dirección ipv4.	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establecer una dirección ipv4.	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 Establecer una dirección ipv4.	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit
Configurar las rutas predeterminadas ipv4 y ipv6 en los puertos seriales	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

2.2.5 Paso 5 configurar swicth 1

En el switch 1 apagamos o desactivamos la búsqueda de DNS. Por otro lado, para poder diferenciar nuestro switch asignamos nombre y contraseña cifrada en modo EXEC y al puerto de consola también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente a nuestro switch configuramos un MOTD Banner.

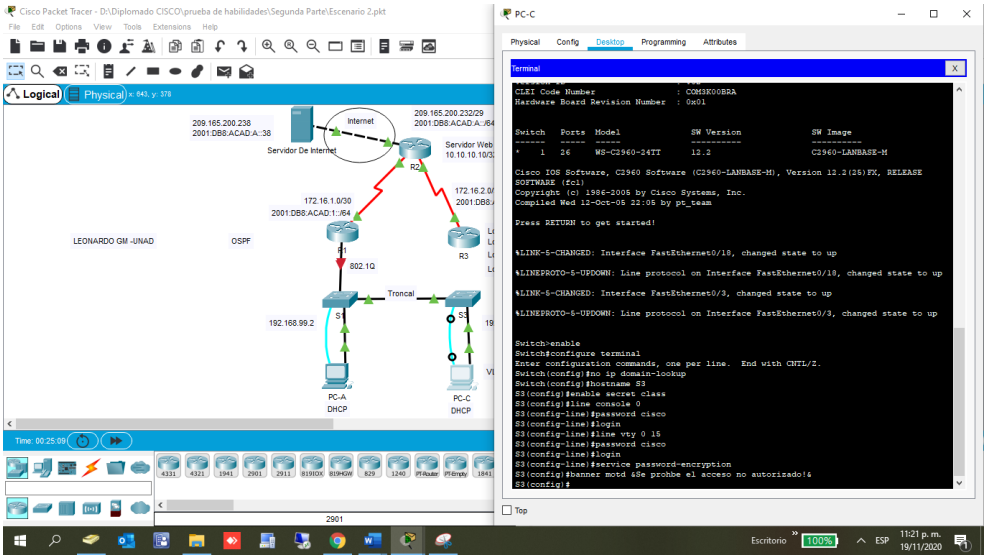
Tabla 17. Configurar S1

Tarea	Especificación
Deshabilitamos la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Asignamos nombre a switch	Switch(config)#hostname S1
Generamos password secreta en modo EXEC	S1(config)#enable secret class
Generamos password de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Configuráramos el inicio en las líneas VTY y generamos password.	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las password de texto.	S1(config)#service password-encryption
Configuramos un MOTD Banner	S1(config)#banner motd &Se prohíbe el acceso no autorizado!&

2.2.6 Paso 6 configurar switch 3

En el switch 3 apagamos o desactivamos la búsqueda de DNS. Por otro lado, para poder diferenciar nuestro switch asignamos nombre y contraseña cifrada en modo EXEC y al puerto de consola también generamos contraseña para que ninguna persona pueda realizar conexiones e ingresar fácilmente a nuestro switch configuramos un MOTD Banner.

Figura 20. configurar switch 3



Fuente: Autor

Tabla 18. Configurar S3

Tarea	Especificación
Deshabilitamos la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Asignamos nombre a switch	Switch(config)#hostname S3
Generamos password secreta en modo EXEC	S3(config)#enable secret class
Generamos password de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Configuráramos el inicio en las líneas VTY y generamos password.	S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las password de texto.	S3(config)#service password-encryption
Configuramos un MOTD Banner	S3(config)#banner motd &Se prohíbe el acceso no autorizado!&

2.2.7 Paso 7 verificar conectividad en la red

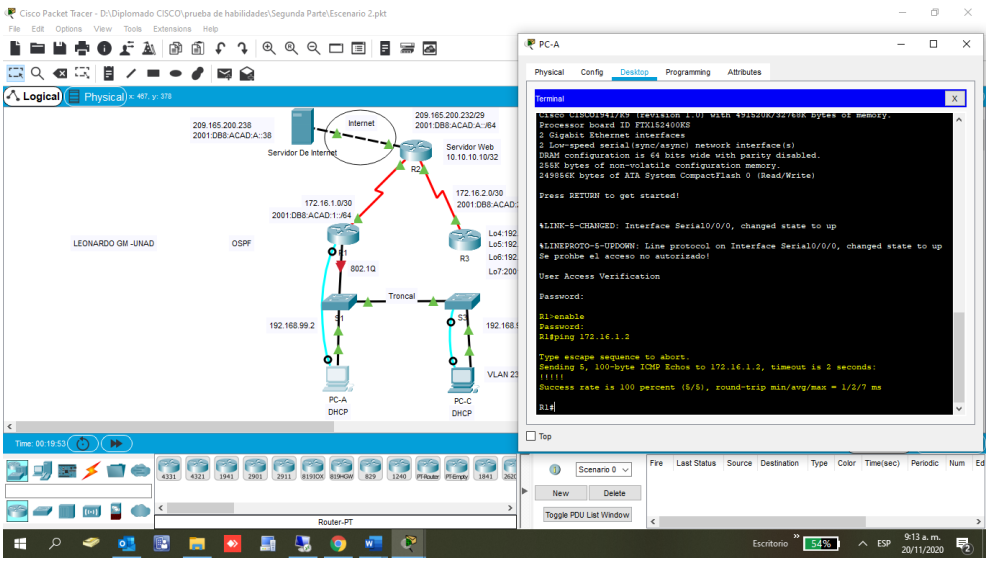
Mediante el comando ping realizamos pruebas de conectividad entre los diferentes dispositivos de la red.

Tabla 19. Verificación de conectividad entre dispositivos

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Success
R2	R3, S0/0/1	172.16.2.1	Success
PC de Internet	Gateway predeterminado	209.165.200.233	Success

Se realiza el ping de verificación desde R1 Hacia R2, S0/0/0

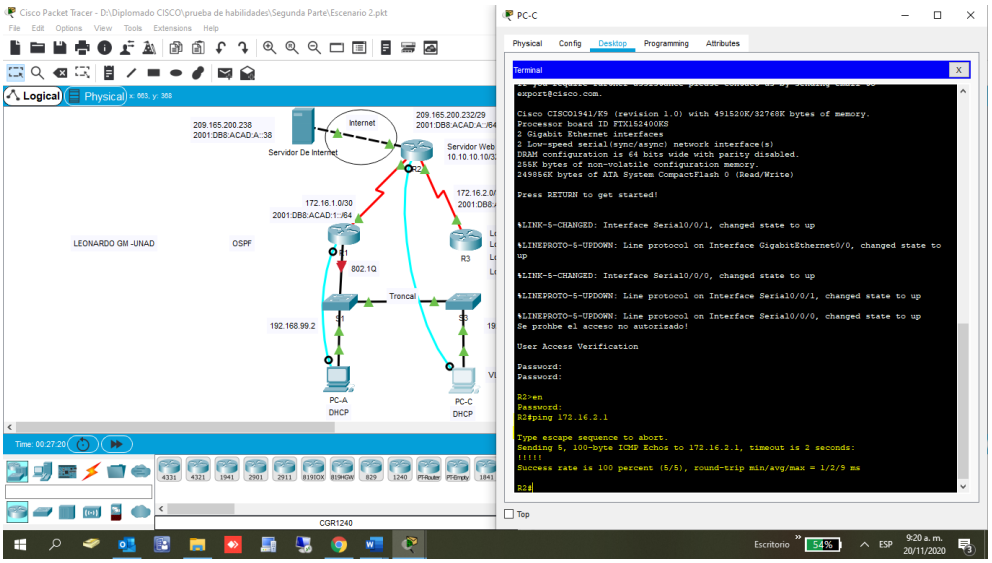
Figura 21. Ping desde R1 Hacia R2, S0/0/0



Fuente: Autor

Se realiza el ping de verificación desde R2 Hacia R3, S0/0/1

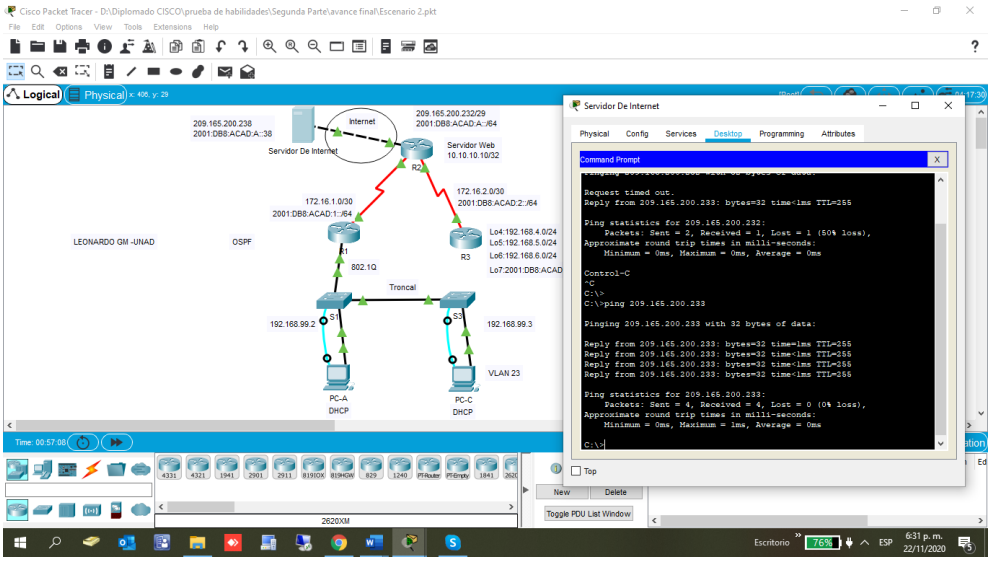
Figura 22. Ping desde R2 Hacia R3, S0/0/1



Fuente: Autor

Se realiza el ping de verificación PC de Internet Hacia Gateway predeterminado

Figura 23. Ping desde PC de Internet Hacia Gateway predeterminado



Fuente: Autor

2.3 Parte 3 configuraciones de seguridad en los switch y routers en las vlan

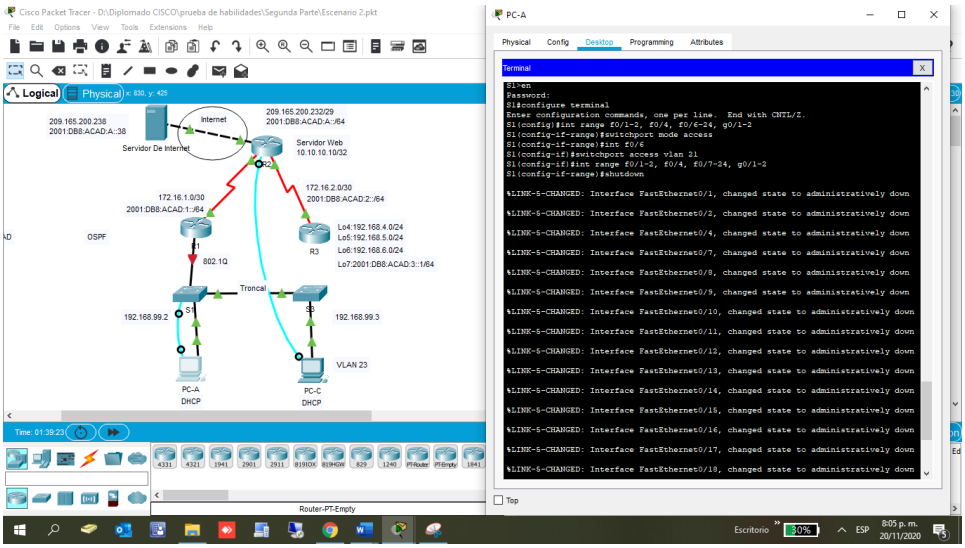
2.3.1 Paso 1 configurar s1

Las configuraciones que realizamos en el switch 1 son las siguientes:

En primer lugar, realizamos la creación de las VLAN y creamos troncos que utilicen las VLAN y configuramos interfaces.

También asignamos el Gateway predeterminado y configuramos la seguridad en los puertos de acceso y algo para tener en cuenta es que en toda configuración debemos proteger las interfaces no utilizadas y asignarlas a determinada VLAN.

Figura 24. Configurar seguridad del Switch 1



Fuente: Autor

Tabla 20. Tareas De Configuracion Del Switch 1

Tarea	Especificación
Creamos las diferentes VLAN	S1(config)#vlan 21 S1(config-vlan)#name Accounting S1(config-vlan)#vlan 23 S1(config-vlan)#name Engineering S1(config-vlan)#vlan 99 S1(config-vlan)#name Management S1(config-vlan)#exit
Asignamos la dirección IPv4 a la VLAN de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Configurar Gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Configurar la troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar la troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar puertos de acceso.	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
configurar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
Apagamos puertos sin usar	S1(config-if-range)# shutdown

2.3.2 Paso 2 configurar s3

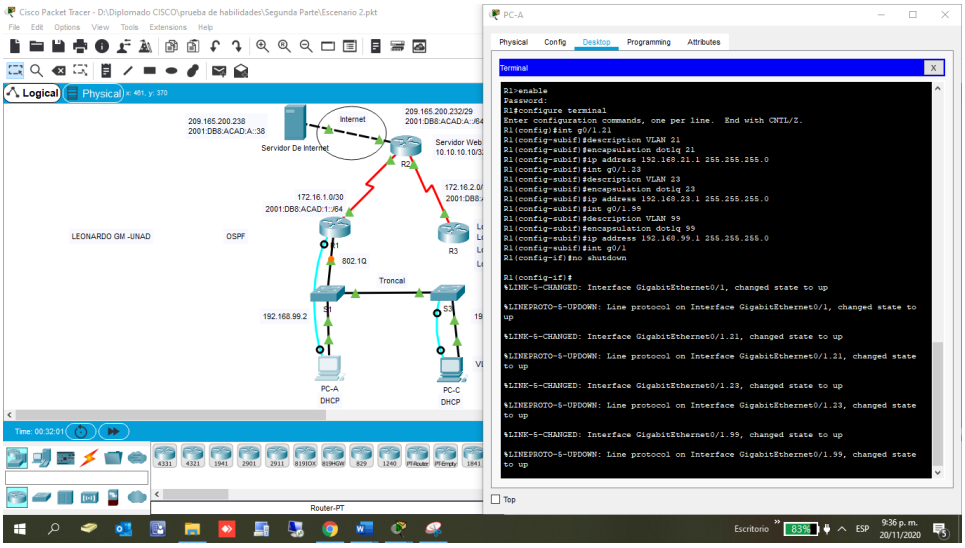
Tabla 21. Tareas De Configuracion Del Switch 3

Tarea	Especificación
Creamos las diferentes VLAN	S3(config)#vlan 21 S3(config-vlan)#name Accounting S3(config-vlan)#vlan 23 S3(config-vlan)#name Engineering S3(config-vlan)#vlan 99 S3(config-vlan)#name Management S3(config-vlan)#exit
Asignamos la dirección IPv4 a la VLAN de administración.	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Configurar Gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Configurar troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configuramos los puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
configurar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#int range f0/1-2, f0/4-17, F0/19-24, g0/1-2
Apagamos puertos sin usar	S3(config-if-range)# shutdown

2.3.3 Paso 3 configurar r1

En esta parte Configuramos la subinterfaz 802.1Q en el router 1 de cada una de las VLAN y activamos la interfaz G0/1 donde asignamos una descripción con el nombre indicado a la subinterfaces y a la VLAN asignada.

Figura 25. configurar r1 subinterfaz 802.1Q



Fuente: Autor

Tabla 22 Tareas De Configuracion Del Router 1

Tarea	Especificación
Configuramos 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configuramos 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)# description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configuramos 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)# description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Habilitamos la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

2.3.4 Paso 4 verificación de conectividad entre los dispositivos

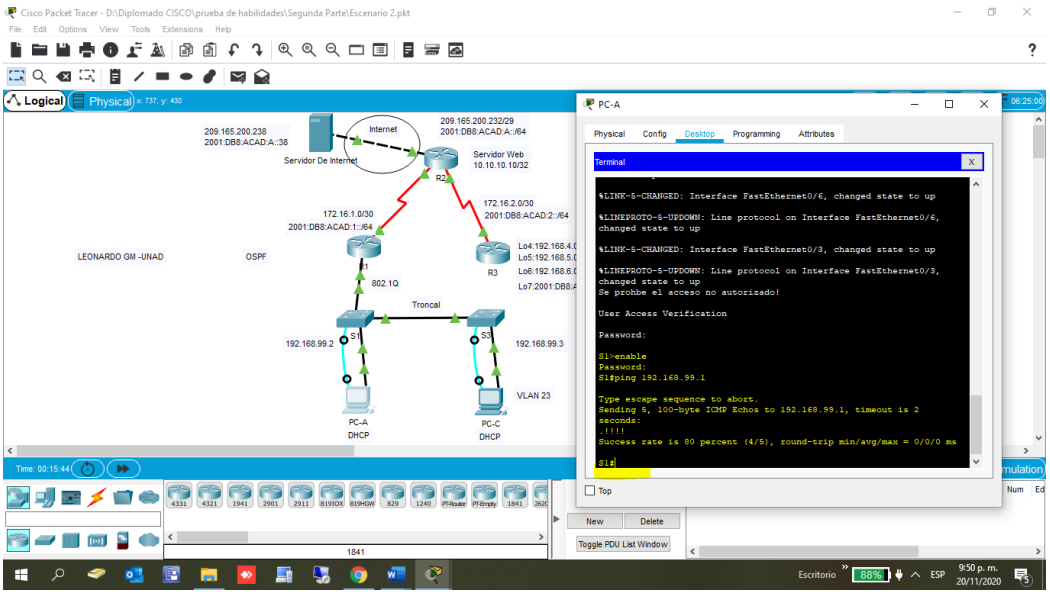
Mediante ping realizamos la validación de conectividad entre los switches y el R1.

Tabla 23. Verificación de conectividad entre los switches y el R1

Desde	A	IP	Resultados
S1	R1, dirección VLAN 99	192.168.99.1	Success
S3	R1, dirección VLAN 99	192.168.99.1	Success
S1	R1, dirección VLAN 21	192.168.21.1	Success
S3	R1, dirección VLAN 23	192.168.23.1	Success

Se realiza el ping de verificación desde S1 Hacia R1, dirección VLAN 99

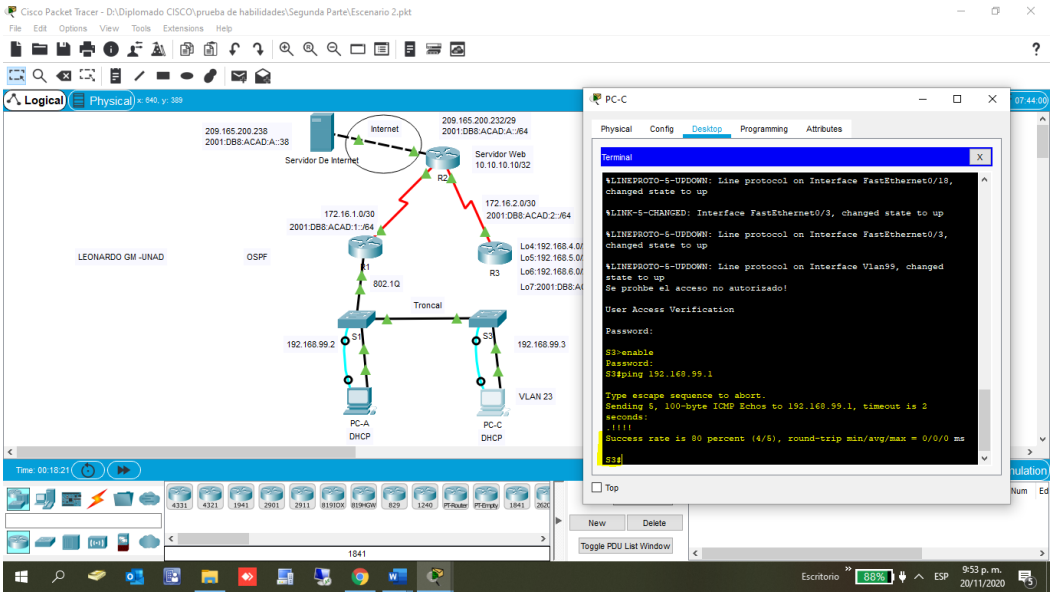
Figura 26. Ping desde S1 Hacia R1, dirección VLAN 99



Fuente: Autor

Se realiza el ping de verificación desde S3 Hacia R1, dirección VLAN 99

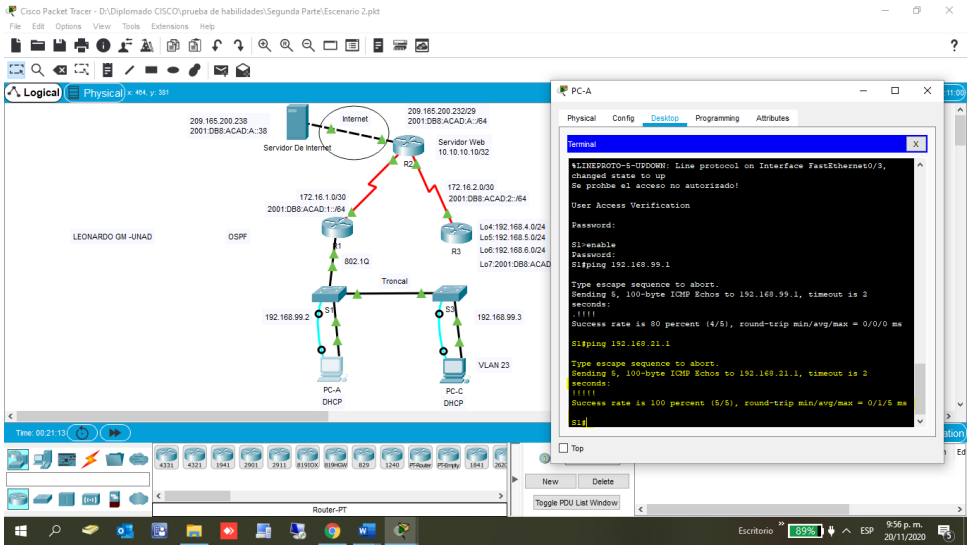
Figura 27. Ping desde S3 Hacia R1, dirección VLAN 99



Fuente: Autor

Se realiza el ping de verificación desde S1 Hacia R1, dirección VLAN 21

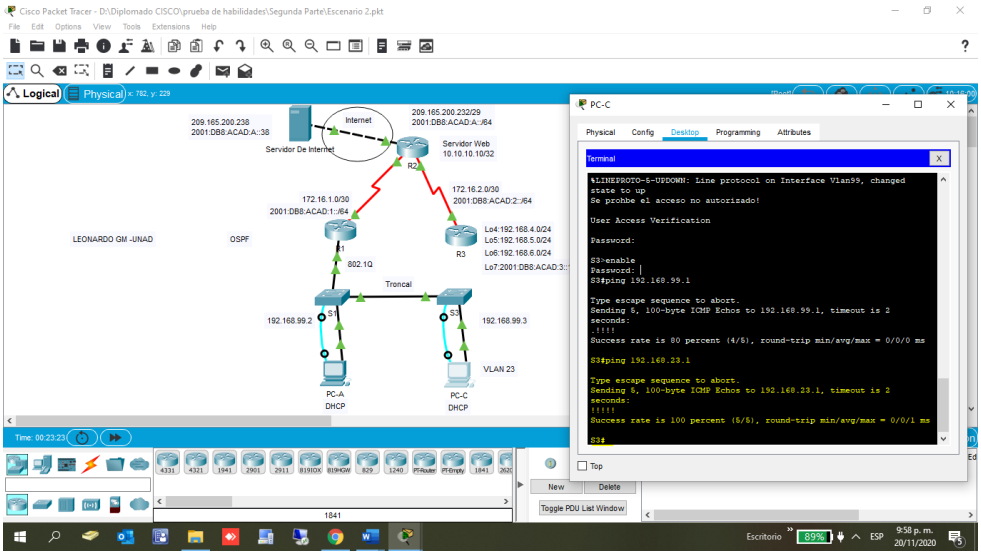
Figura 28. Ping desde S1 Hacia R1, dirección VLAN 21



Fuente: Autor

Se realiza el ping de verificación desde S3 Hacia R1, dirección VLAN 23

Figura 29. Ping desde S3 Hacia R1, dirección VLAN 23



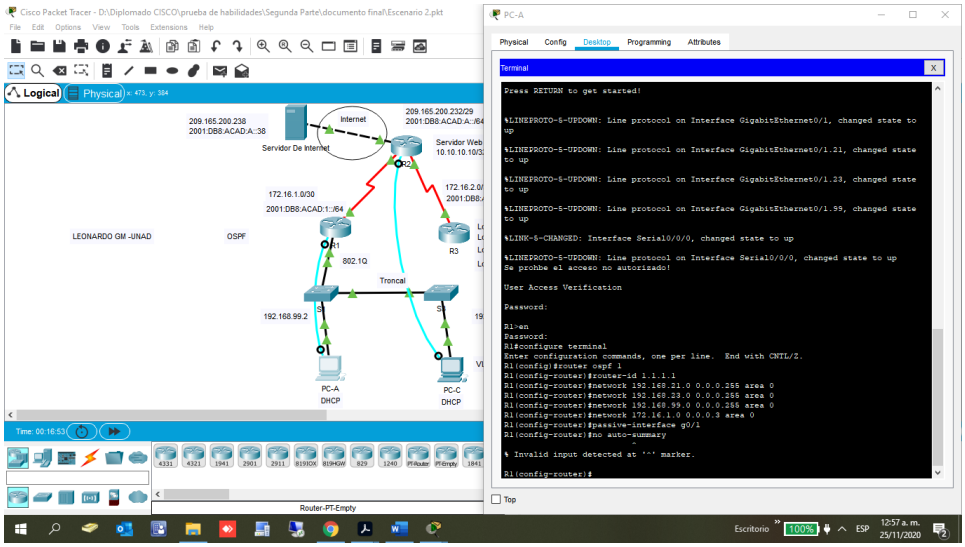
Fuente: Autor

2.4 parte 4 configuraciones de protocolo routing dinámico OSPF

2.4.1 paso 1 configurar OSPF en r1

En el router 1 configuramos el protocolo OSPF y del área 0 en la topología de red en donde se muestran todas la redes conectadas directamente y se establece todas las interfaces LAN como pasivas y automáticamente se desactiva la sumarizacion.

Figura 30. configurar OSPF en r1



Fuente: Autor

Tabla 24. Configurar OSPF en el R1

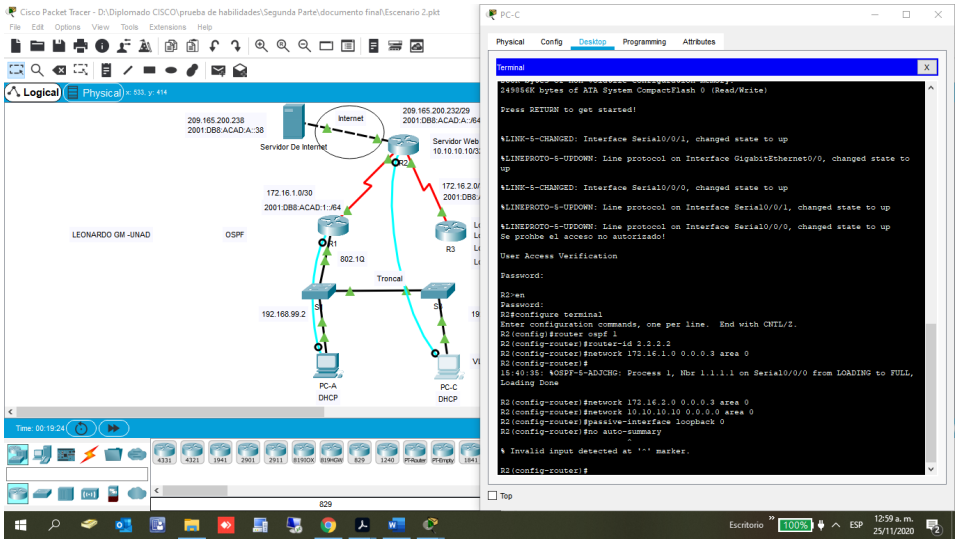
Tarea	Especificación
Configuramos OSPF en área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Asignar redes conectadas directamente	R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0

Establecer interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1
Desactivar sumarización	R1(config-router)#no auto-summary

2.4.2 Paso 2 configurar OSPF en r2

En el router 2 configuramos el protocolo OSPF y del área 0 en la topología de red en donde se muestran todas la redes conectadas directamente descartando la interface GigabitEthernet0/0 se establece todas las interfaces LAN loopback como pasivas y automáticamente se desactiva la sumarizacion.

Figura 31. configurar OSPF en r2



Fuente: Autor

Tabla 25. Configurar OSPF en el R2

Tarea	Especificación
Configuramos OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2

Asignar redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface loopback 0
Desactivar sumarización	R2(config-router)#no auto-summary

2.4.3 Paso 3 configurar ospfv3 en r3

En el router 3 configuramos el protocolo OSPFv3 y configurar prefijos con ipv6 del área 0 en la topología de red en donde se muestran todas la redes conectadas directamente con ipv4, se establece todas las interfaces LAN piv4 loopback como pasivas y automáticamente se desactiva la sumarizacion.

Tabla 26. Configurar OSPF en el R3

Tarea	Especificación
Configuramos OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Configuramos OSPFv3 área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 33.33.33.33 R3(config-rtr)#passive-interface default R3(config-rtr)#exit R3(config)#interface s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config)#interface loopback 7 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#exit

Asignar redes conectadas directamente	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 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer 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
Desactivar sumarización.	R3(config-router)#no auto-summary

2.4.4 Paso 4 verificación información OSPF

Verificamos que OSPF esté funcionando correctamente mediante los comandos de CLI.

Tabla 27. Verificar Informacion De OSPF

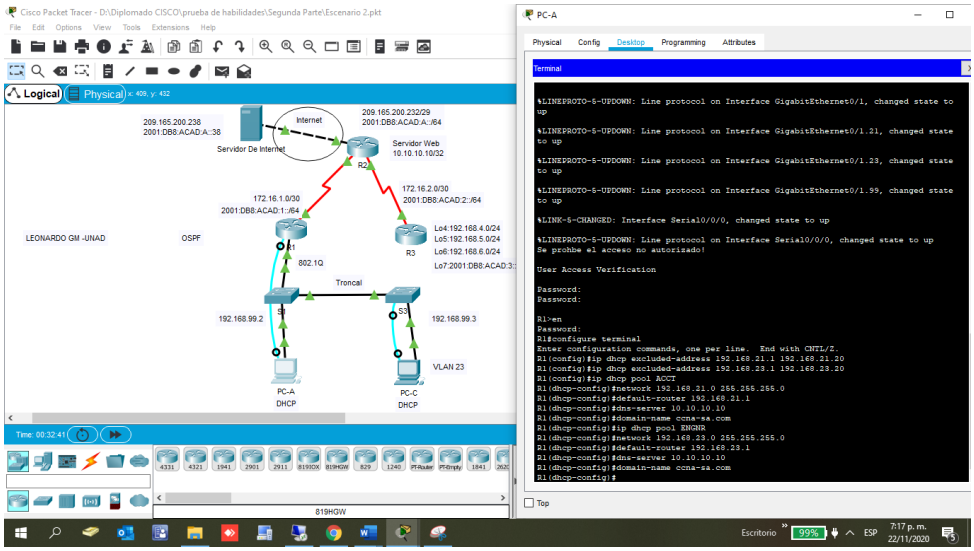
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2# show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2# show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2# show run | section router OSPF

2.5 Parte 5 implementación de DHCP y NAT para ipv4

2.5.1 Paso 1 configurar r1 en vlan 21,23

En el router r1 creamos un pool DHCP de las VLAN 21 y 23 con un nombre para ser identificados en la red LAN, las direcciones del servidor DNS, el nombre del dominio.

Figura 32. configurar r1 en vlan 21,23



Fuente: Autor

Las configuraciones para R1 son las siguientes:

Tabla 28. Configurar R1 Como DHCP Para VLAN 21 y 23

Tarea	Especificación
Reservamos las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservamos las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Creamos un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

Creamos un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

2.5.2 Paso 2 configurar NAT estática y dinámica en r2

En el router 2 creamos una base de datos local con nombre de usuario y habilitamos el servicio HTTP y definimos el pool de direcciones públicas utilizables y la traducción de direcciones de red NAT.

Tabla 29. Configurar NAT En R2

Tarea	Especificación
Creamos una base de datos local con una cuenta de Usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar servicio HTTP	R2(config)#ip http server
Configurar HTT para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
Asignamos interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configuramos la NAT dinámica dentro de una ACL privada	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 0.0.3.255

Definimos el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definimos la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

2.5.3 Paso 3 verificación del protocolo DHCP y la NAT

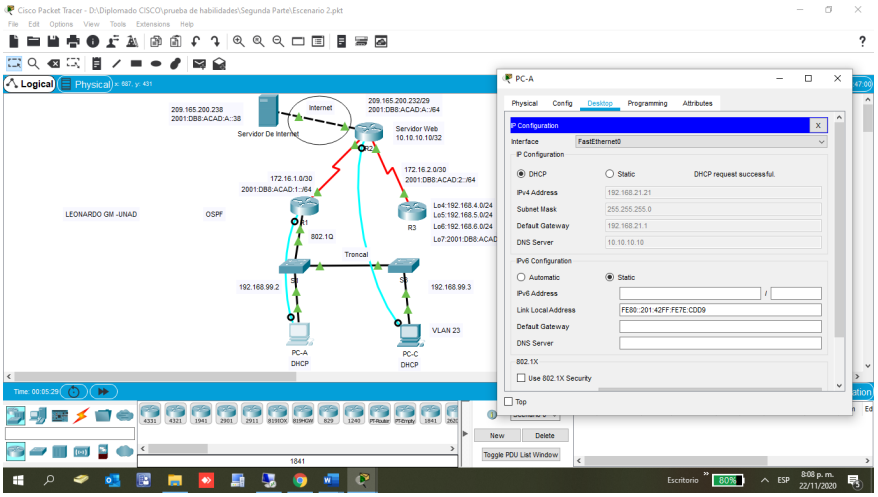
Realizamos las pruebas de conectividad del protocolo DHCP y la NAT entre cada uno de los diferentes dispositivos para obtener resultados satisfactorios.

Tabla 30. Verificación De Protocolo DHCP Y NAT

Prueba	Resultados
Verificamos que la PC-A haya adquirido información de IP del servidor de DHCP	Success
Verificamos que la PC-C haya adquirido información de IP del servidor de DHCP	Success
Verificamos que la PC-A pueda hacer ping a la PC-C	Success
accedemos al servidor web	Success

Verificamos que PC-A haya adquirido información de IP del servidor de DHCP

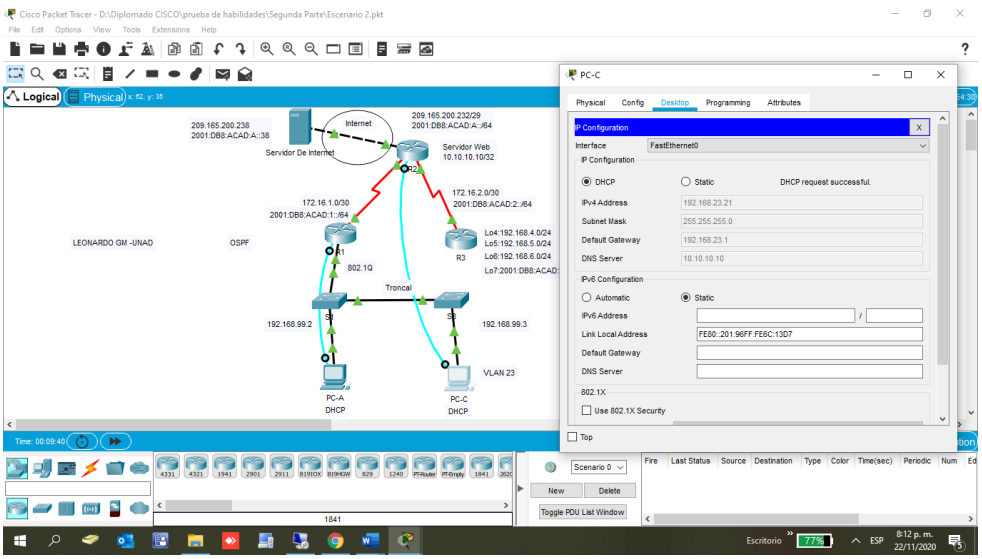
Figura 33. Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



Fuente: Autor

Verificamos que PC-C haya adquirido información de IP del servidor de DHCP

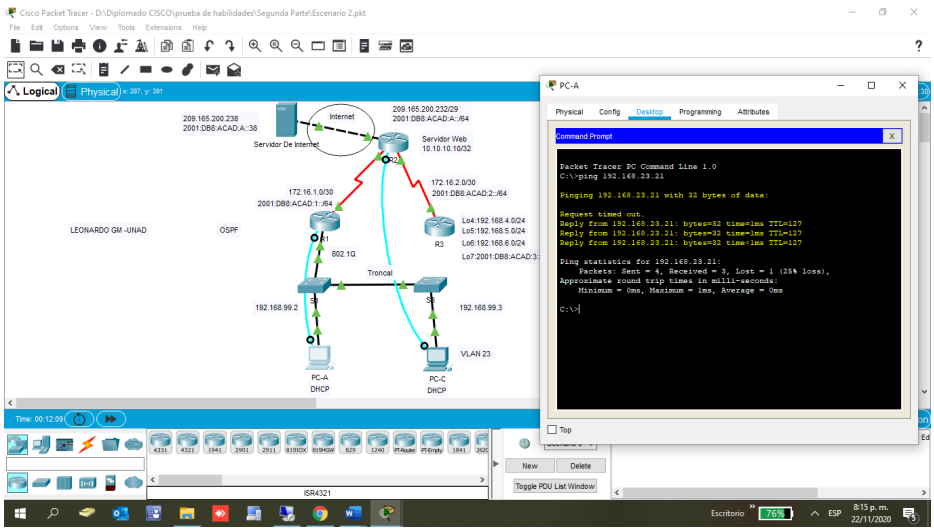
Figura 34. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP



Fuente: Autor

Verificamos que la PC-A pueda hacer ping a la PC-C

Figura 35.Verificar que la PC-A pueda hacer ping a la PC-C



Fuente: Autor

2.6 Parte 6 configuración de NTP

En el router 2 ajustamos fecha y hora y dejamos r2 como un maestro NTP y configuramos R1 como cliente NTP y se valida la respectiva configuración.

Tabla 31. Configurar NTP

Tarea	Especificación
Ajustar la fecha y hora en R2.	R2#clock set 08:50:00 22 november 2020
Configuramos R2 como un maestro NTP.	R2#configure terminal R2(config)#ntp master 5
Configuramos R1 como un cliente NTP.	R1#configure terminal R1(config)#ntp server 172.16.1.2
Configuramos R1 para update de calendario.	R1(config)#ntp update-calendar R1(config)#end
Validamo la configuración de NTP en R1.	R1#show ntp associations

2.7 Parte 7 configuración y validación de lista de acceso ACL

2.7.1 Paso 1 restringir acceso a vty en r2

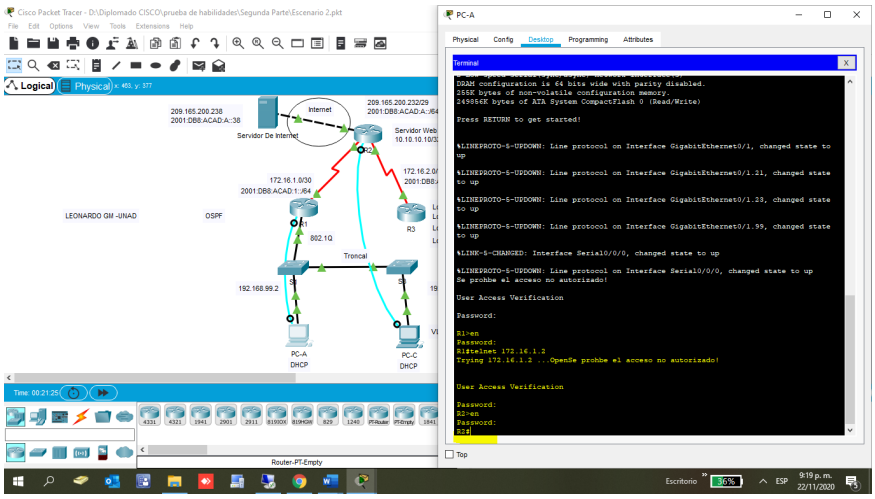
Realizamos la configuración de una lista de acceso con el respectivo nombre para que solo r1 establezca una conexión con r2 asignado una ACL y permisos de acceso mediante telnet con nombre a las líneas VTY validando el funcionamiento.

Tabla 32. Configurar Las Listas (ACL)

Tarea	Especificación
Configuramos lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2#configure terminal R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicamos ACL con nombre a las líneas VTY	R2(config)#line vty 0 15
Permitimos acceso a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet
Validamos que ACL funcione correctamente	R1#telnet 172.16.1.2

Verificamos que la ACL funcione como se espera

Figura 36. Verificar que la ACL funcione como se espera



Fuente: Autor

2.7.2 Paso 2 verificar el comando CLI para mostrar información

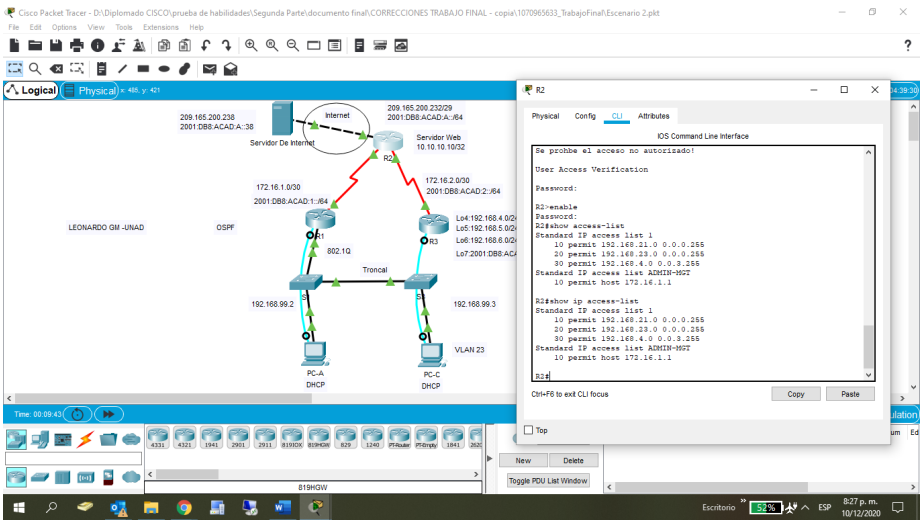
Validamos con algunos comando CLI la información de r2 en donde mostramos las coincidencias recibidas por una lista de acceso desde la última vez que se restableció, con qué comando se muestran las traducciones NAT y que comando se utiliza para eliminar las traducciones de NAT dinámicas.

Tabla 33. Comandos CLI

Descripción	Comando
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2# show access-list R2# show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations

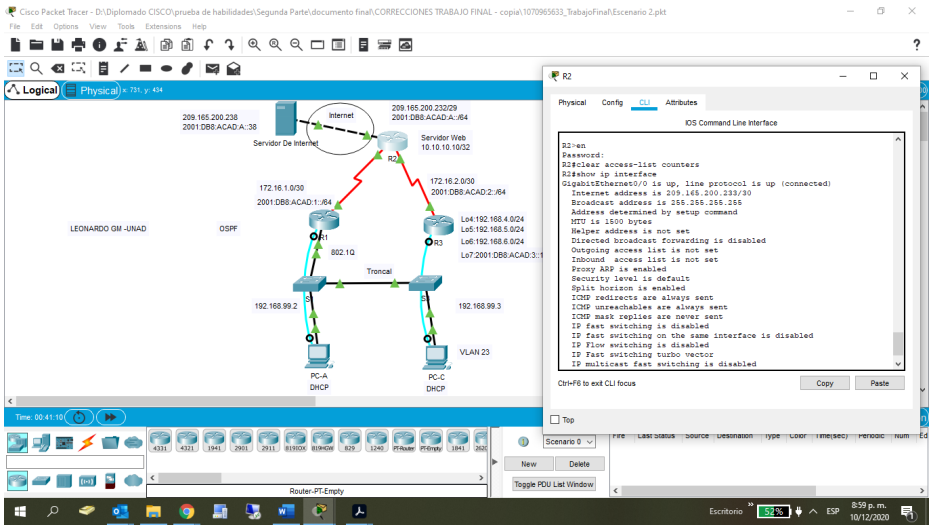
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Figura 37. Comando show access-list



Fuente: Autor

Figura 38. Comando show ip interface



Fuente: Autor

CONCLUSIONES

En diplomado de profundización CISCO se logró conocer las configuraciones y funciones que requiere un router y switch para tener una correcta administración en una red donde en el escenario 1 se aplicaron las configuraciones básicas y direccionamiento ipv4 e ipv6 y se logró comprender como se realiza la administración de seguridad en cada uno de los switch y router, entre cada una de las VLAN y su enrutamiento DHCP. En el escenario 2 se aplicaron los enrutamientos OSPF, protocolos y VLAN e implementación NAT de los diferentes dispositivos, configuración de servidor web y las lista de control ACL y el protocolo NTP, para la implementación de políticas de seguridad y acceso.

En cuanto a la solución de los ejercicios propuestos en el diplomado de profundización CISCO CCNA, se desarrollaron en totalidad cumpliendo con el paso a paso de los puntos propuestos mediante el software de simulación Packet Tracer, validando fallas y verificación de conectividad entre los diferentes dispositivos, analizando cada uno de los protocolos y métricas de enrutamiento en la red.

BIBLIOGRAFIA

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

(ECBTI Sala 6_391, n.d.)ECBTI Sala 6_391. (n.d.). Retrieved October 20, 2020, from http://conferencia2.unad.edu.co/physutq52uzf/?proto=true

(Teoria « Todo sobre Packet Tracer, n.d.)Teoria « Todo sobre Packet Tracer. (n.d.). Retrieved October 20, 2020, from https://todopacketracer.com/category/redes/teoria/

ANEXOS

ANEXO 1

Enlace de descarga de archivo de simulación del escenario 1 diseñado en packet tracer:

https://drive.google.com/drive/folders/1kF5-tPOFB-hE1zpk-x8mfxG0ane3cUhi?usp=sharing

ANEXO 2

Enlace de descarga de archivo de simulación del escenario 2 diseñado en packet tracer:

https://drive.google.com/drive/folders/1lsn-iND0FZ1SRlrlKO1k4aFxUB80n61f?usp=sharing

ANEXO 3

Articulo

SOLUCIÓN DE UNA TOPOLOGIA DE RED BAJO EL USO DE TECNOLOGÍA CISCO

Jose Leonardo Garcia Martinez
Universidad Nacional Abierta y A distancia UNAD, jlgarciamar@unadvirtual.edu.co

Resumen

En el desarrollo del escenario uno se diseña y se configura una red pequeña en el software de simulación packet tracer y se realizan las configuraciones básicas y protocolos de enrutamientos entre VLAN, DHCP y EtherChannel para cada uno de los diferentes dispositivos para las redes LAN mediante el modelo de referencia OSI. Los router y switch están diseñados para que en la configuración se admita conectividad tanto por ipv4 como por ipv6 ya que las direcciones ipv4 están agotadas con el avance de la tecnología y el internet de las cosas haciendo que cada día más personas utilicen más aparatos electrónicos y estén conectados a INTERNET. En el escenario se muestran que los resultados son claves y fundamentales ya que se estos dispositivos admiten la actualización de este protocolo IP en pro de un mejor funcionamiento de la red LAN. Es de gran importancia realizar una correcta administración de la red por medio de estas actualizaciones y configuraciones de seguridad para que podamos contar con redes más seguras y estables, garantizando así una mejor conexión.

Palabras clave: (ipv6, router, switch, vlan, dhcp, EtherChannel, LAN)

Abstract:

In the development of scenario one, a small network is designed and configured in the packet tracer simulation software and the basic configurations and routing protocols between VLAN, DHCP and EtherChannel are indicated for each of the different devices for the LAN networks through the OSI reference model. Routers and switches are designed so that the configuration supports both ipv4 and ipv6 connectivity since ipv4 addresses are exhausted with the advancement of technology and the internet of things, causing more and more people to use an electronic device and are connected to the INTERNET. The scenario shows that the results are key and fundamental since these devices support the update

of this IP protocol in favor of a better functioning of the LAN network. It is of great importance to carry out a
correct administration of the network through these updates and security configurations so that we can have more secure and stable networks, thus guaranteeing a better connection.

Keywords: (ipv6, router, switch, vlan, dhcp, EtherChannel, LAN)

I. Introducción

El diseño y configuración de la topología de red se realiza mediante el software de simulación packet tracer donde se utilizan los siguientes dispositivos. Un router con referencia **[1]** Cisco 2911 que ofrece un servicio de aplicaciones, voz, video y datos altamente seguros y dos switches **[2]** Cisco Catalyst 3560-X Series los cuales soportan una base IP y servicios IP y cuentan con un nuevo conjunto de funciones LAN Base, acceso a Capa 2 y 3 funciones de servicios IP avanzado y conmutación Layer 3 donde soporta (IPv4 e IPv6). También se utilizan dos equipos de cómputo. Una vez conectados los dispositivos correctos se procede a cargar la plantilla sdm prefer en los switch para que soporten IPv6.

También debemos tener presente que el router y los switch se deben administrar de forma segura, configurando el enrutamiento entre **[3]** VLAN mediante el envió de tráfico de una VLAN a otra. Para que estas puedan establecer comunicación entre ellas deben ser necesarios los servicios de un router. Para esto se

establecen Subinterfaces FastEthernet, encapsulación y dirección IP correspondiente de manera que cada una de estas pertenezca a un vlan determinada.
Muchas veces es necesario agrupar usuarios de la misma Vlan que se encuentran ubicados en diferentes zonas, para establecer una comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las vlan que tienen configuradas a través de enlaces troncales y en algunas ocasiones utilizar el **[4]** EtherChannel para sumar la velocidad de cada puerto físico para obtener un enlace troncal o ancho de banda de alta velocidad.

[5]El DHCP permite asignar automáticamente direcciones IP reutilizables a clientes asignando direccionamiento a los host de un rango preconfigurado. Con**[6]**el port-security creamos una política de seguridad de capa 2, para evitar conexiones no deseadas a los equipos host o puertos. La activación de Port Security se debe realizar a nivel de interfaz y para ello debemos deshabilitar el modo auto que viene configurado por defecto en todos los puertos de un switch y configurar estos puertos como [7] access que permite pasar solo una Vlan, los paquetes no van etiquetados, y por lo general se usa para conectar dispositivos finales y trunk que permite manejar el tráfico de distintas Vlan en un mismo puerto, que cada paquete irá etiquetado y cuando se envíe a una vlan se podrá resolver correctamente. Este tipo de configuración se usa para interconectar distintos tipos de equipos de red, como pueden ser 2 switches en la red. Se desarrollo esta actividad de una manera completa, validando fallas y verificación de conectividad entre los diferentes dispositivos, analizando cada uno de los protocolos y métricas de enrutamiento en la red.

II METODOLOGIA

Este trabajo se desarrolla mediante la investigación aplicada y se emplea un modelo para poder probar la conectividad tanto de IPv4 como de IPv6 entre todos los dispositivos de la [8] topología de red que sabemos que es la que realiza la (interconexión de nodos). La investigación está diseñada para verificar metódicamente la conectividad con cada dispositivo de la red y donde se puedan tomar las medidas correctivas para establecer la conectividad si esta presenta alguna falla con algún dispositivo o equipos host. Estas conexiones entre dispositivos se realizan con un tipo de cable de cobre de par trenzado para red de área local llamado en el simulador de packet tracer **[9]** Copper straight-through (LAN) uso para el que los conectores RJ-45 en cada extremo. Es idéntico al cruce del cable , excepto que en este último los alambres en el cable se cruzan de manera que el recibir pernos de la señal en el conector en un extremo están conectados a los pernos de la señal de transmisión en el conector en el otro extremo.

Esta validación de conectividad se realiza por el comando ping Para comprobar la disponibilidad de un ordenador, **[10]**Ping que envía, en la configuración estándar, cuatro paquetes de solicitud de eco ICMP de 32 bytes donde este protocolo sirve para intercambiar información y avisos de error en redes IPv4. **[11]**Para las redes de ordenadores basadas en IPv6, está disponible el protocolo sucesor ICMPv6 que debe estar completamente incorporada en todas las implementaciones y nodos IPv6.

Algo clave es saber que el **[12]** método experimental nos ayuda para la recolección de datos en el cual se comparan las mediciones y estos se evidencia en el objetivo de este escenario que es validar que todos los dispositivos puedan conectarse a todos los recursos de red de una manera correcta y rápida.

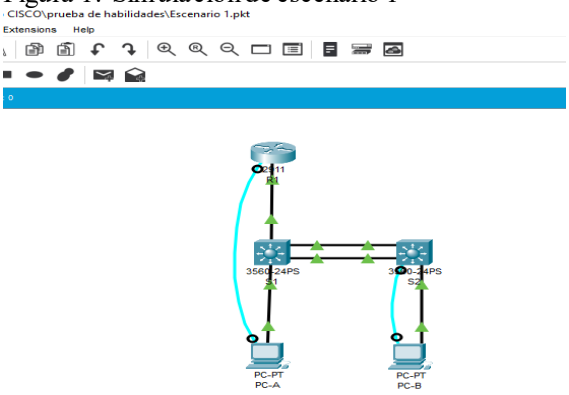
Como sabemos los router y switch están diseñados para mantener una comunicación al nivel de la capa 2, capa 3 y capa 4 del modelo **[13]** OSI para mantener una correcta conectividad y administración de dichos dispositivos en nuestra topología para que estos utilicen DHCP para IPv4 y se asigne estáticamente las direcciones IPv6 y se utilice también el Link Local.

Sabemos que nuestra plantilla [14] SDM funciona con el protocolo IPv6 ya que ayuda al conmutador a administrar la asignación de recursos de cada característica. Hay algunas características que están deshabilitadas en la plantilla predeterminada. Entonces, si queremos trabajar con estas características, debemos habilitarlas desde la interfaz de línea de comandos **[15]** (CLI) de Cisco IOS que es la interfaz de usuario principal que se utiliza para configurar, monitorear y mantener los dispositivos de Cisco. Esta interfaz de permite ejecutar directa y simplemente comandos de Cisco IOS, ya sea usando una consola o terminal de enrutador, o usando métodos de acceso remoto.

III RESULTADOS

En esta topología de red se indican una serie de configuraciones para lo dispositivos de red las cuales se deben realizar en cada equipo para obtener los resultados de conectividad deseados en cada uno de los dispositivos.

Figura 1. Simulación de escenario 1



Para la verificación de la conexión en cada uno de los dispositivos de indican una serie de configuraciones a realizar en cada dispositivo como los son los nombres cada una de las VLAN.

Tabla 1. Nombres de vlan

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

Luego tenemos la tabla de direcciones para cada dispositivo.

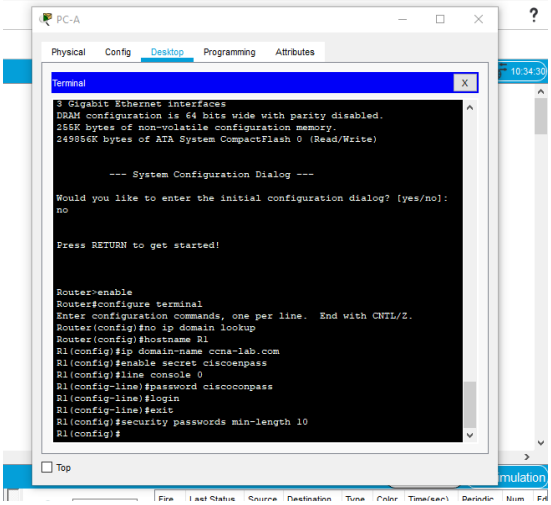
Tabla 2. Asignación de direcciones.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1/26	No corresponde
	2001:db8:acad:a::1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65/27	No corresponde
	2001:db8:acad:b::1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97/29	No corresponde
	2001:db8:acad:c::1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1/27	No corresponde
	2001:db8:acad:209::1 /64	No corresponde
S1 VLAN 4	10.19.8.98/29	10.19.8.97
	2001:db8:acad:c::98 /64	No corresponde
	fe80::98	No corresponde
S2 VLAN 4	10.19.8.99/29	10.19.8.97
	2001:db8:acad:c::99 /64	No corresponde
	fe80::99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b::50 /64	fe80::1

Para una correcta administración de estos dispositivos es clave la configuraciones y seguridad en cada equipo con asignación de contraseña cifrada en modo EXEC y

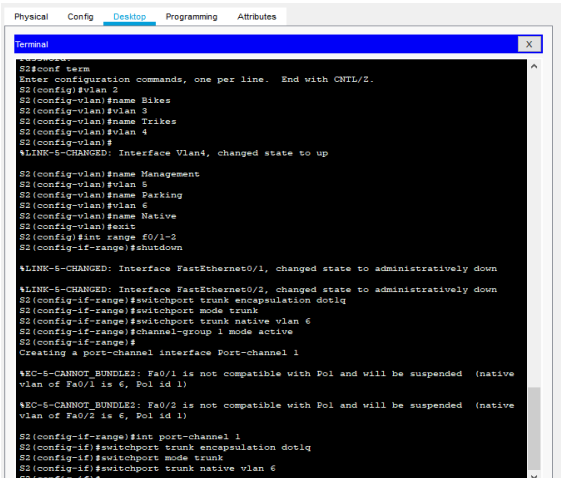
al puerto de consola para que ninguna persona pueda realizar conexiones e ingresar fácilmente. Es importante configurar el inicio de sesión en las líneas VTY para poder acceder a nuestros dispositivo a través de Telnet, pero esto solo aceptando y habilitando el router ipv6 y cada una de las interfaces. Se genera una clave de cifrado RSA para una mayor seguridad en nuestros equipos.
Por otro lado, para poder diferenciar cada uno de nuestros equipos asignamos nombre y se ingresa a un dominio.

Figura 2. Configuracion dispositivo



Son creadas las VLAN y se crean troncos que utilicen la VLAN nativa y se configuran cada una de las interfaces. También se crea un grupo de puertos EtherChannel y los puertos de acceso de host y la seguridad en los puertos de acceso a direcciones MAC y se protegen las interfaces o puertos no utilizadas y se asigna na determinada VLAN.

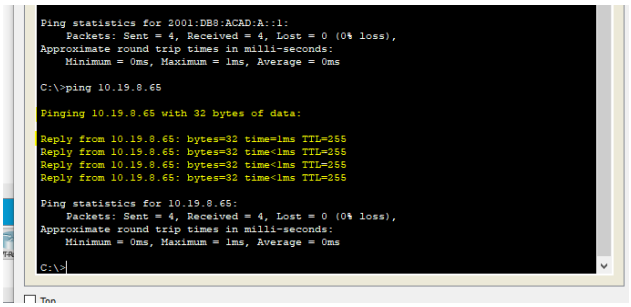
Figura 3. Creación VLAN



Para poder asegurar una correcta administración de nuestra topología de red LAN debemos validar las configuraciones en cada uno de nuestros dispositivos para ellos utilizamos nuestro comando de ping para validar la conectividad IPv4 e IPv6 entre todos los dispositivos de nuestra red. Algo positivo en la configuración de la red es que todos los ping entre los diferentes dispositivos respondieron satisfactoriamente para lograr la configuración total de en la topología de red.

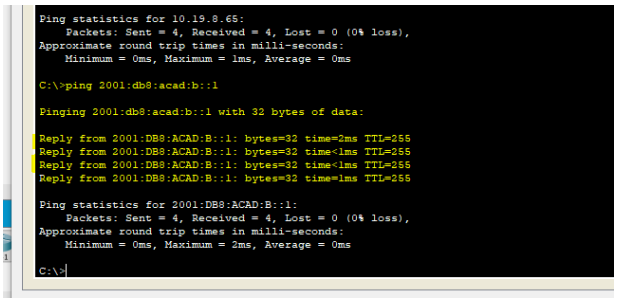
Realizamos la respectiva verificación de conectividad mediante ping desde nuestro PC-A Hacia R1 - 10.19.8.65

Figura 4. Ping desde PC-A Hacia R1 - 10.19.8.65



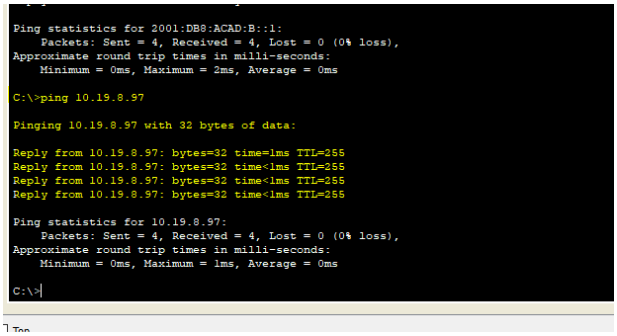
Realizamos la respectiva verificación de conectividad mediante ping desde PC-A Hacia R1 - 2001:db8:acad:b::1

Figura 5. Ping desde PC-A Hacia R1 - 2001:db8:acad:b::1



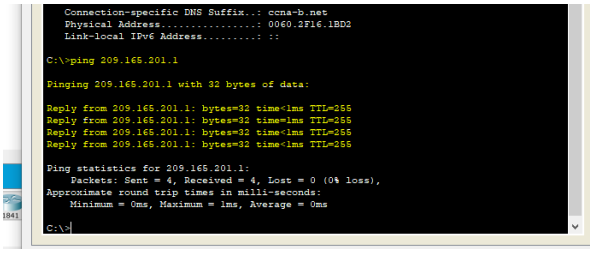
Realizamos la respectiva verificación de conectividad mediante ping desde PC-A Hacia R1 - 10.19.8.97

Figura 6. Ping desde PC-A Hacia R1 - 10.19.8.97



Realizamos la respectiva verificación de conectividad mediante ping desde PC-B Hacia R1 – 209.165.201.1

Figura 7. Ping desde PC-B Hacia R1 – 209.165.201.1



IV CONCLUSIONES

En cuanto a la solución la topología de red del escenario 1 mediante la simulación en packet tracer se desarrolló en totalidad cumpliendo con el paso a paso de los puntos propuestos, en donde se aplicaron las configuraciones básicas para cada uno de los dispositivos y direccionamiento ipv4 y ipv6, enrutamientos de los protocolos y VLAN y se realizó ping de conectividad entre cada uno, para una correcta administración y seguridad en la red .

V REFERENCIAS

[1] Enrutador de servicios integrados Cisco 2911 - Cisco. (n.d.). Retrieved November 26, 2020, from https://www.cisco.com/c/en/us/products/routers/2911-integrated-services-router-isr/index.html

[2] Switch Cisco Catalyst Administrable capa L3 con 24 puertos GigE 350W, 4 x 10G SFP + 2 x 10BG SFP Uplinks - WS-C3560X-24T-S. (n.d.). Retrieved November 26, 2020, from http://ds3comunicaciones.com/cisco/WS-C3560X-24T-S.html

[3] Aprende Redes.com » Enrutamiento entre Vlans. (n.d.). Retrieved November 26, 2020, from https://aprenderedes.com/2020/02/enrutamiento-entre-vlans/

[4] Soluciones con EtherChannel de capa 2 | GT Raul Flores. (n.d.). Retrieved November 26, 2020, from https://eduaraul15.wordpress.com/2010/01/10/soluciones-con-etherchannel-de-capa-2/

[5] Configuración dinámica de opciones del servidor DHCP - Cisco. (n.d.). Retrieved November 26, 2020, from https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

[6] ¿Cómo Implementar Port Security? – Mira Telecomunicaciones. (n.d.). Retrieved November 26, 2020, from https://miratelecomunicacions.com/blog/noticias-cisco/como-implementar-port-security-2/

[7] Parte 13 – Puerto en modo Access vs Trunk | NKSistemas. (n.d.). Retrieved November 27, 2020,

from https://nksistemas.com/parte-13-puerto-en-modo-access-vs-trunk/

[8] Tipos de Topología de red: malla, estrella, árbol, bus y anillo | Explicación. (n.d.). Retrieved November 27, 2020, from https://www.locurainformaticadigital.com/2018/07/17/topologia-de-red-malla-estrella-arbol-bus-anillo/

[9] LUIS CARLOS GALAN SARMIENTO: PACKET TRACER. (n.d.). Retrieved November 27, 2020, from http://estructura28-37.blogspot.com/2016/07/packet-tracer.html

[10] Comando Ping | Diagnóstico de red en Windows - IONOS. (n.d.). Retrieved November 27, 2020, from https://www.ionos.es/digitalguide/servidores/herramientas/comando-ping/

[11] 7. ICMP en IPv6 - Redes locales y globales. (n.d.). Retrieved November 27, 2020, from https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/7-icmp-en-ipv6

[12] Método experimental (Psicología). (n.d.). Retrieved November 27, 2020, from https://glosarios.servidor-alicante.com/psicologia/metodo-experimental.

[13] *MODELO OSI - INFRAESTRUCTURA DE RED*. (n.d.). Retrieved November 27, 2020, from https://sites.google.com/site/estandaresred/tipos-de-red/modelo-osi

[14] Cómo habilitar el soporte de IPv6 en un Switch Cisco catalisys 3560 - Red10Education. (n.d.). Retrieved November 27, 2020, from https://red10education.com/blog/como-habilitar-el-soporte-de-ipv6-en-un-switch-cisco-catalisys-3560/.

[15] Guía de configuración de los fundamentos de la configuración, versión 15M & T de Cisco IOS: mediante la interfaz de línea de comandos de Cisco IOS [Cisco IOS 15.4M & T] - Cisco. (n.d.). Retrieved November 27, 2020, from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/cf-cli-basics.html

BIOGRAFÍA

Leonardo Garcia Martinez (N'1992) nació en Santa Fe de Bogotá Colombia , el 28 de octubre de 1992. Se graduó del instituto nacional de aprendizaje SENA, en Mosquera - Cundinamarca, y actualmente cursa un grado de estudio a nivel superior en la Universidad Nacional Abierta y a Distancia UNAD.

Su experiencia profesional incluye la compañía Discovery Farms, Alcaldía de Facatativá y Corpoica **(Corporación Colombiana de Investigación Agropecuaria).** Sus áreas de interés incluyen, entre otras, las de desarrollo de software y seguridad informática. En el momento no cuenta con grados honorarios pero su meta es con el tiempo recibir algunos de estos reconocimientos.