

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

YEIMY LORENA CUVIEDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTÁ
2020

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

YEIMY LORENA CUVIEDES

Diplomado de opción de grado presentado para
optar el título de INGENIERA DE SISTEMA

DIRECTOR:
MSc. DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA INGENIERIA SISTEMAS
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 10 de noviembre de 2020

AGRADECIMIENTOS

A mi madre principalmente por confiar más en mí incluso en los momentos donde ni yo misma confiaba. A la memoria de mi padre, por enseñarme más con su ejemplo que con su palabra.

CONTENIDO

INTRODUCCIÓN	12
OBJETIVOS	13
Escenario 1	14
Topología	14
La Tabla 1 muestra la información de VLAN que se configurará.	14
<i>Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos</i>	15
Paso 1: Inicializar y volver a cargar el router y el switch	15
Paso 2: Configurar R1	19
Paso 3: Configure S1 y S2.....	28
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)....	33
Paso 4: Configurar S1.....	33
Paso 5: Configure el S2.	38
Parte 2: Configurar soporte de host	42
Paso 1: Configure R1.....	42
Paso 2: Configurar los servidores	45
Parte 3: extremo	46
Escenario 2	58
Parte 1:Inicializar dispositivos	58
Parte 2: Configurar los parámetros básicos de los dispositivos	61
Parte 2:Configurar la seguridad del switch, las VLAN y el routing entre VLAN	69
Paso 3 . Configurar el protocolo de routing dinámico OSPF	75
Parte 3:Implementar DHCP y NAT para IPv4	77
Parte 4:Configurar NTP.....	81
Parte 5:Configurar y verificar las listas de control de acceso (ACL).....	82
CONCLUSIONES	86
BIBLIOGRAFÍA	87

LISTA DE TABLAS

Tabla 1. Tabla de VLANS	15
Tabla 2. PC-A a Router/Switch	16
Tabla 3. De PC-B a S1	18
Tabla 4. Configuración S2	18
Tabla 5. Tabla de configuración Router	22
Tabla 6. Tabla de configuración Router	23
Tabla 7. Configurar interfaz.....	23
Tabla 8. Tabla R1 G0/0/1.3.....	24
Tabla 9. R1 G0/0/1.4.....	25
Tabla 10. R1 G0/0/1.6.....	26
Tabla 11. R1 Loopback0.....	27
Tabla 12. Confiración S1 y S2	30
Tabla 13. Clave de cifrado RSA.....	30
Tabla 14. Gateway predeterminado	31
Tabla 15. S1 VLAN 4	31
Tabla 16. S2 VLAN 4	32
Tabla 17. Crear VLAN.....	33
Tabla 18. Troncos 802.1Q	34
Tabla 19. Puertos EtherChannel.....	35
Tabla 20. Puerto de acceso de host.....	36
Tabla 21. Seguridad del puerto.....	36
Tabla 22. Interfaces no utilizadas.....	37
Tabla 23. Crear VLAN.....	38
Tabla 24. VLAN 6 nativa	39
Tabla 25. Port-security en los access	41
Tabla 26. Configure Default Routing	43
Tabla 27. IPv4 DHCP para VLAN 2	43
Tabla 28. DHCP IPv4 para VLAN 3	44
Tabla 29. Ejecución de pruebas ping	56
Tabla 30. Pruebas ping.....	57
Tabla 31. Comando de inicializar dispositivos.....	60
Tabla 32. Tarea de configuración	61
Tabla 33. Tarea de configuración	62
Tabla 34. R1 Config.....	63
Tabla 35. Configuración R2	65
Tabla 36. Configuración R3	66
Tabla 37. Configuración R1	67
Tabla 38. Configuración S3.....	68
Tabla 39. Conectividad de la red	68
Tabla 40. Configuración S1 y Routing.....	70
Tabla 41. Configuración del S3.....	71
Tabla 42. Configurar R1.....	73
Tabla 43. Conectividad de la red	74
Tabla 44. OSPF en el R1	75
Tabla 45. Configurar OSPF en el R2	75
Tabla 46. Tarea de configuración	76
Tabla 47. Verificación OSPF.....	77
Tabla 48. R1 como servidor de DHCP	78
Tabla 49. NAT estática y dinámica.....	79

Tabla 50. Protocolo DHCP y la NAT	81
Tabla 51. Configurar NTP	81
Tabla 52. Líneas VTY en el R2	82
Tabla 53. Comando de CLI	84

LISTA DE FIGURAS

Figura 1. Topología de Escenario 1	14
Figura 2. Simulación en Packet Tracer	15
Figura 3. configuración de PC-A a R1.....	17
Figura 4. Configuración PC-B	17
Figura 5. Borrado datos de Vlan	18
Figura 6. Configuración.....	19
Figura 7. Se confirma que S1 y S2 soporta IPv6.....	19
Figura 8. Tabla de direccionamiento aplicados	22
Figura 9. Se configura: R1 G0/0/1.2.....	24
Figura 10. Se configura R1 G0/0/1.3.....	25
Figura 11. Se configura R1 G0/0/1.4.....	26
Figura 12. Se configura R1 G0/0/1.6.....	27
Figura 13. R1 Loopback0.....	28
Figura 14. Clave de cifrado RSA.....	28
Figura 15. Configuración de las tareas	30
Figura 16. Clave de cifrado RSA.....	31
Figura 18. Configuración direccionamiento.....	32
Figura 19. S2 VLAN 4 configurado.....	33
Figura 20. VLAN creadas.....	34
Figura 21. Troncos 802.1Q	35
Figura 22. Grupo de puertos EtherChannel	35
Figura 23. Grupo de puertos EtherChannel	36
Figura 24. Puerto en los puertos de acceso.....	37
Figura 25. Protección de interfaces.....	38
Figura 26. Crear VLAN	39
Figura 27. Troncos 802.1Q	40
Figura 28. Puertos EtherChannel de Capa 2	40
Figura 29. Puerto de acceso del host.....	41
Figura 30. Port-security en los access ports	41
Figura 31. Interfaces no utilizadas	42
Figura 32. Activación	42
Figura 33. Configuración Default Routing	43
Figura 34. IPv4 DHCP para VLAN 2	44
Figura 35. DHCP IPv4 para VLAN 3	45
Figura 36. Host PC-A y PC-B.....	45
Figura 37. PC-A y PC-B.....	46
Figura 38. 10.19.8.99.....	47
Figura 39. 10.19.8.99.....	47
Figura 40. IP address will vary.....	48
Figura 41. 2001:db8:acad:b: :50	49
Figura 42. 2001:db8:acad:b: :50	49
Figura 43. 209.165.201.1	50
Figura 44. 2001:db8:acad:209: :1	50
Figura 45. 209.165.201.1	51
Figura 46. 2001:db8:acad:209: :1	51
Figura 47. 10.19.8.1.....	52
Figura 48. 2001:db8:acad:a: :1	52
Figura 49. 10.19.8.65.....	53
Figura 50. 2001:db8:acad:b: :1	53

Figura 51. 10.19.8.97.....	54
Figura 52. 2001:db8:acad:c: :1	54
Figura 53. 10.19.8.98.....	55
Figura 54. 2001:db8:acad:c: :98	55
Figura 55. 10.19.8.99.....	56
Figura 56. 2001:db8:acad:c: :99	56
Figura 57: Topología escenario 2.....	58
Figura 58: Topología del escenario.....	58
Figura 59. Tarea Comando de IOS	60
Figura 60. Ejecución no shutdown	61
Figura 61. Configuración del R2us.....	65
Figura 62. Conectividad de la red	68
Figura 63. Conectividad de la red aplicada	69
Figura 64. Configurar el S3.....	72
Figura 65. Configurar R1	73
Figura 66. Conectividad de la red	74
Figura 67. Configurar OSPF en el R2	76
Figura 68. Información de IP del servidor de DHCP.....	80
Figura 69. IP del servidor de DHCP	80
Figura 70. PC-A pueda hacer ping a la PC-C	81
Figura 71. Navegador web.....	81
Figura 72. NTP en R1	82
Figura 73. NTP en R1	83
Figura 74. Comando de CLI.....	84
Figura 75. Comando de CLI.....	85

GLOSARIO

CISCO SYSTEMS: Empresa global principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

TOPOLOGÍA: Es la rama de las matemáticas dedicada al estudio de aquellas propiedades de los cuerpos geométricos que permanecen inalteradas por transformaciones continuas, disciplina que estudia las propiedades de los espacios topológicos y las funciones continuas.

INTERFAZ: Son las rutas que se establecen de datos y toman vía los destinos particulares.

VTP: VTP (VLAN Trunking Protocol) es un protocolo de propiedad de Cisco utilizado por los conmutadores de Cisco para intercambiar información de VLAN.

RESUMEN

A continuación se desarrollan dos escenarios planteados como pruebas de habilidades prácticas cada una exige los métodos aprendidos en el desarrollo para la solución de problemas, en el escenario uno debemos elaborar una relación entre los diferentes así como los comandos utilizados y la salida de estos, a su vez se debe realizar una codificación con los parámetros establecidos, por su parte en el escenario dos se tiene que configurar los Switches mientras se verifica los como clientes, además de repetir los procedimientos en los puertos propuestos.

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

ABSTRACT

Next, two scenarios proposed as practical skills tests are developed, each one requires the methods learned in the development for solving problems, in scenario one we must develop a relationship between the different as well as the commands used and the output of these, to in turn, a coding must be carried out with the established parameters, for its part, in scenario two, the switches must be configured while they are verified as clients, in addition to repeating the procedures on the proposed port.

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

INTRODUCCIÓN

A continuación, usando los diferentes programas de simulación se describen paso a paso la configuración de los dispositivos de cada escenario, se exhibe su correcta operación ayudado de los comandos respectivos que permiten evidenciar su operatividad tanto en la utilización de protocolos, en el intercambio de información de sistemas autónomos, como la distribución de mediante el protocolo.

OBJETIVOS

OBJETIVO GENERAL.

Aplicar cada uno de los conocimientos adquiridos a lo largo de la realización del diplomado de Cisco CCNA LAN WAN, se realizará una resolución completa de dos escenarios en los que se deben aplicar las distintas configuraciones bajo los requerimientos que brinda la guía de actividades.

OBJETIVOS ESPECÍFICOS.

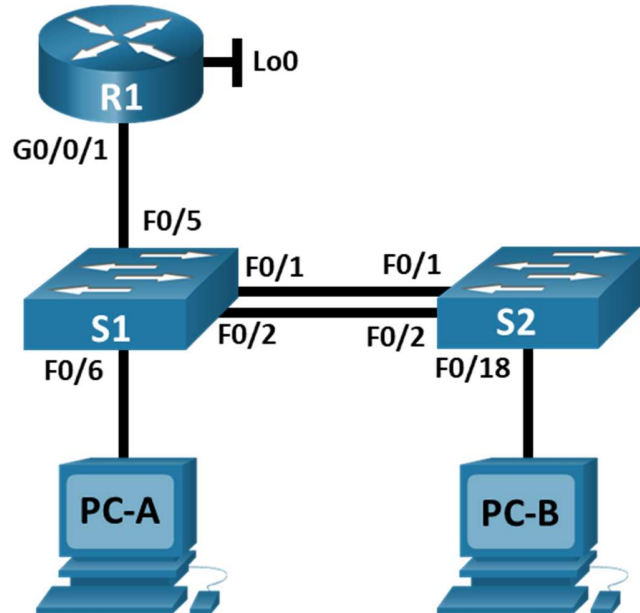
Identificar el proceso de configuración que se debe aplicar a los escenarios asignados.

Realizar configuraciones respectivas en Packet Tracer, efectuar los ajustes que sean necesarios teniendo en cuenta los escenarios planteados.

Escenario 1

Topología

Figura 1. Topología de Escenario 1



Fuente: Documento del Repositorio

La figura 1 muestra la topología a desarrollar dentro del escenario 1

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

La Tabla 1 muestra la información de VLAN que se configurará.

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

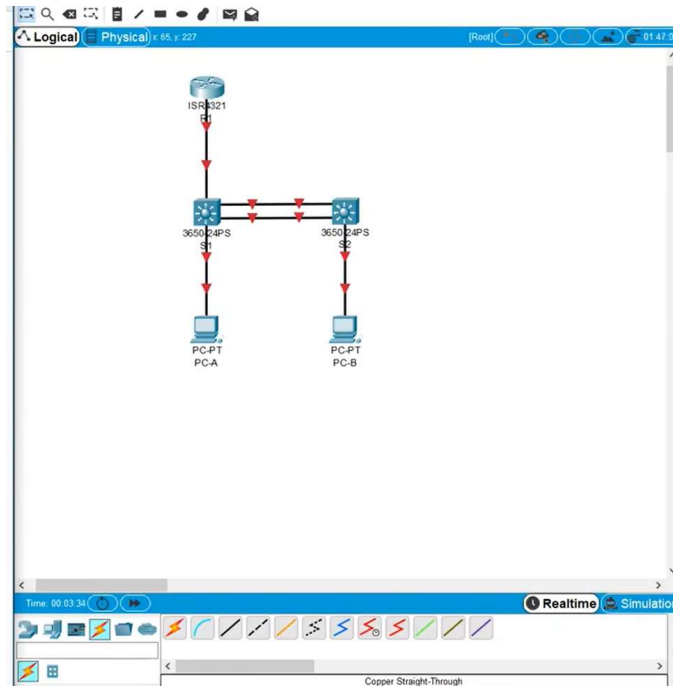
Tabla 1. Tabla de VLANS

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos

Figura 2. Simulación en Packet Tracer



Fuente: Autor

En la figura 2 se analiza el escenario modelado en el programa en el cual se partirá para ejecutar los pasos y las interfaces correspondientes

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

Tabla 2. Asignación de direcciones

La tabla 2 las direcciones a asignar a cada dispositivo. Esta tabla siempre debe completarse antes de comenzar a configurar el dispositivo, y esta tabla debe completarse teniendo en cuenta los requisitos de topología.

```

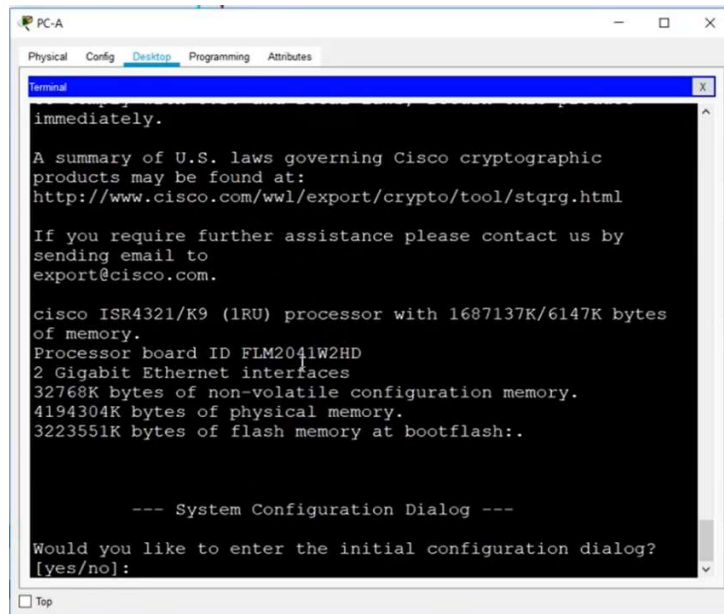
Router/Switchs >enable
Router/Switchs #erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router/Switchs #reload
System configuration has been modified. Save? [yes/no]:yes

```

Tabla 3. PC-A a Router/Switch

En la tabla 3 se utiliza el cable de la consola para conectarse desde la PC-A a Router/Switch (puerto de consola) se va desde PC-A a Router, Switch1, Switch 2

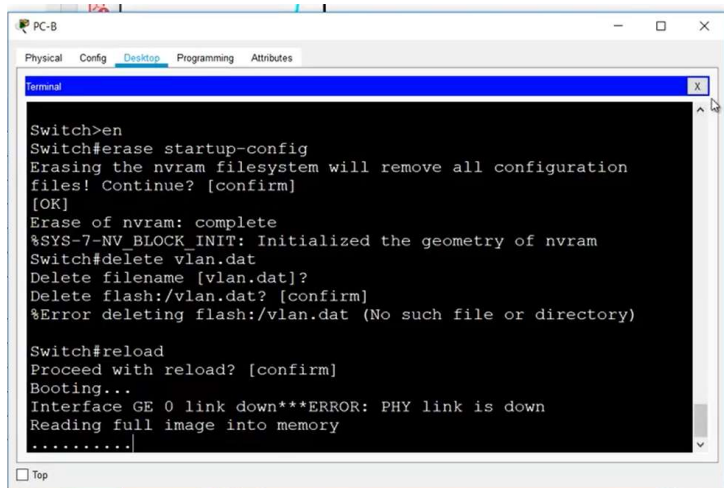
Figura 3. configuración de PC-A a R1



Fuente: Autor

En la figura 3 se analiza que el router no tiene configuraciones de inicio, listo para usarse.

Figura 4. Configuración PC-B



Fuente: Autor

En la Figura 4 se realiza la configuración del PC-B siguiendo los pasos asignados y configuración del Switch

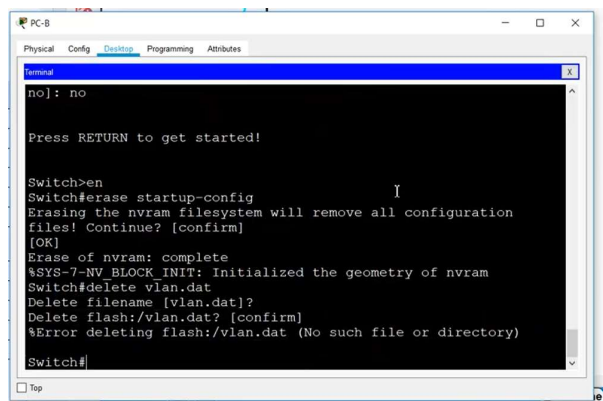
Switch(config)# **sdm prefer dual-ipv4-and-ipv6 default**

```
Switch(config)# exit  
Switch# reload  
Proceed with reload? [confirm]
```

Tabla 4. De PC-B a S1

En la tabla 4 podemos analizar los comandos Switch SDM los cuales fueron configurados y se anexó y recargó.

Figura 5. Borrado datos de Vlan



```
PC-B  
Physical Config Desktop Programming Attributes  
Terminal  
no]: no  
  
Press RETURN to get started!  
  
Switch>en  
Switch#erase startup-config  
Erasing the nvram filesystem will remove all configuration  
files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram  
Switch#delete vlan.dat  
Delete filename [vlan.dat]?  
Delete flash:/vlan.dat? [confirm]  
%Error deleting flash:/vlan.dat (No such file or directory)  
Switch#
```

Fuente: Autor

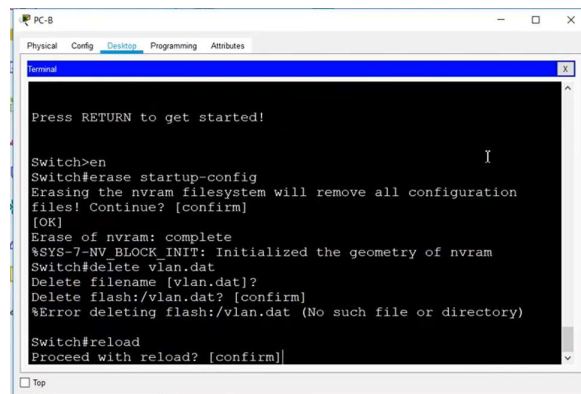
Se selecciona: No, se aplica la configuración al Switch correspondiente y relacionada a la tabla 5, esta hace parte de la configuración aplicada a S2

Configuración S2

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default  
Switch(config)# exit  
Switch# reload  
Proceed with reload? [confirm]
```

Tabla 5. Configuración S2

Figura 6. Configuración



```
PC-8
Physical Config Desktop Programming Attributes
Terminal
Press RETURN to get started!

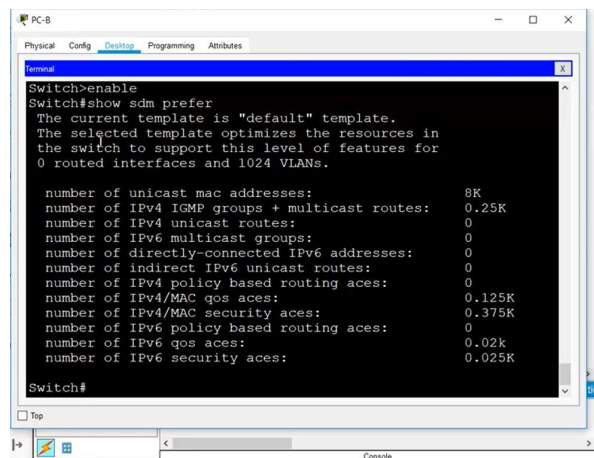
Switch>en
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
```

Fuente: Autor

En la figura 6 se analiza que después de recargar el switch, configura la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch. El Sdm prefer

Figura 7. Se confirma que S1 y S2 soporta IPv6



```
PC-8
Physical Config Desktop Programming Attributes
Terminal
Switch>enable
Switch#show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 1024 VLANs.

number of unicast mac addresses:          8K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes:           0
number of IPv6 multicast groups:         0
number of directly-connected IPv6 addresses: 0
number of indirect IPv6 unicast routes:  0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces:             0.125K
number of IPv4/MAC security aces:        0.375K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces:                 0.02k
number of IPv6 security aces:            0.025K

Switch#
```

Fuente: Autor

En la Figura 7 se ve como tanto el S1 como el S2 soporta el protocolo IPv6.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router R1	Router#config t Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1#config t R1(config)#enable secret ciscoenpass
Contraseña 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	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1#config t R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#config t R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Este es un sistema seguro. Solo acceso autorizado" R1(config)#exit
Habilitar el routing IPv6	R1#config t R1(config)#ipv6 unicast-routing

<p>nfigurar interfaz G0/0/1 y subinterfaces</p>	<pre> R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Interface Vlan2 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-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Interface Vlan3 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-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description Interface Vlan6 Native R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#no shutdown R1(config- subif)#exit R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Interface Vlan4 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-subif)#no shutdown </pre>
---	--

Tarea	Especificación
Configure el Loopback0 interface	R1(config)#interface loopback 0 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)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024

Tabla 6. Tabla de configuración Router

En la tabla 6 están cada una de las configuraciones del router específicas para cada una de las configuraciones reflejando los comandos usados en la configuración del enrutador, los comandos ejecutados en el dispositivo durante la entrada.

DESARROLLO

Figura 8. Tabla de direccionamiento aplicados

```

Router>
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoconpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin secret adminlpass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd %Unauthorized Access is Prohibited!%
R1(config)#ipv6 unicast-routing
R1(config)#

```

Fuente: Autor

En la Figura 8 se aplican los direccionamientos en router y R1 aplicando los diferentes ítems aplicando cada una de las indicaciones de la tabla.

En esta fase se utiliza la tabla de direccionamiento:

Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1
----------------------------------	---

Tabla 7. Tabla de configuración Router

En la tabla 7 se configura el Loopback0 interface, La interfaz de bucle invertido es una interfaz virtual. Siempre que al menos una de las interfaces IP del conmutador esté operativa, siempre se podrá acceder a ella. Por lo tanto, la interfaz loopback es útil para depurar, porque si hay otras interfaces, siempre puede hacer ping a su dirección IP. Interruptor activo

Tabla de direccionamiento:

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

Tabla 8. Configurar interfaz

En la tabla 8 se ve como se configura la interfaz y se nota que los enlaces no corresponden

Configurar interfaz G0/0/1 y subinterfaces

Figura 9. Se configura: R1 G0/0/1.2

```

Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin secret adminlpass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd %Unauthorized Access is Prohibited!%
R1(config)#ipv6 unicast-routing
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-subif)#
    
```

Fuente: Autor

En la figura 9 se la hace la configuración R1 G0/0/1.2 en todos los R1 paso a paso

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde

Tabla 9. Tabla R1 G0/0/1.3

En la tabla 9 corresponde a R1 G0/0/1.3 se analiza que la puerta de enlace predeterminada no corresponde.

Figura 10. Se configura R1 G0/0/1.3

```

R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-length 10
R1(config)#username admin secret adminpass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd %Unauthorized Access is Prohibited!%
R1(config)#ipv6 unicast-routing
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-subif)#int g0/0/1.3
R1(config-subif)#encapsulation dot1q 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-subif)#
    
```

Fuente: Autor

En la figura 10 podemos ver cómo Se configura R1 G0/0/1.3 en los aspectos de encapsulation, se asigna ip adres y se comprueba el IPv6

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde

Tabla 10. R1 G0/0/1.4

En la tabla 10 se muestra que la interfaz R1 G0/0/1.4 su puerta de enlace predeterminada el enlace no corresponde y esta es la que se aplica al R1

Figura 11. Se configura R1 G0/0/1.4

```

R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd %Unauthorized Access is Prohibited!%
R1(config)#ipv6 unicast-routing
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-subif)#int g0/0/1.3
R1(config-subif)#encapsulation dot1q 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-subif)#int g0/0/1.4
R1(config-subif)#encapsulation dot1q 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-subif)#
    
```

Fuente: Autor

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.6	No corresponde	No corresponde

Tabla 11. R1 G0/0/1.6

Figura 12. Se configura R1 G0/0/1.6,

```

PC-A
Physical Config Desktop Programming Attributes
Terminal
R1(config)#ipv6 unicast-routing
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-subif)#int g0/0/1.3
R1(config-subif)#encapsulation dot1q 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-subif)#int g0/0/1.4
R1(config-subif)#encapsulation dot1q 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-subif)#int g0/0/1.6
R1(config-subif)#encapsulation dot1q 6 native
R1(config-subif)#description Native
R1(config-subif)#int g0/0/1
R1(config-if)#
  
```

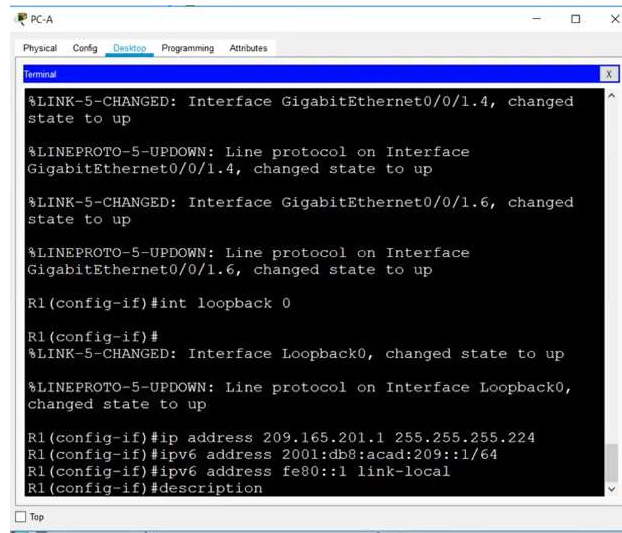
Fuente: Autor

En la figura 12 se aplica la configuración al R1 aplicando lo R1 G0/0/1.6

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde

Tabla 12. R1 Loopback0

Figura 13. R1 Loopback0

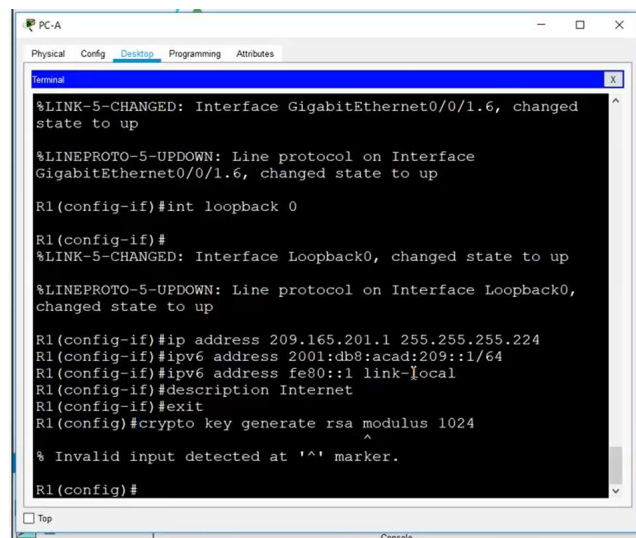


```
PC-A
Physical Config Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.4, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.4, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.6, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.6, changed state to up
R1(config-if)#int loopback 0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
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
```

Fuente: Autor

En la figura 13 se nota como no corresponde la puerta de enlace predeterminada con respecto al R1 Loopback0 teniendo en cuenta la dirección IP.

Figura 14. Clave de cifrado RSA



```
PC-A
Physical Config Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.6, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1.6, changed state to up
R1(config-if)#int loopback 0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
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 Internet
R1(config-if)#exit
R1(config)#crypto key generate rsa modulus 1024
^
% Invalid input detected at '^' marker.
R1(config)#
```

Fuente: Autor

En la figura 14 se nota como se genera una clave de cifrado RSA: Módulo de 1024 bits

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

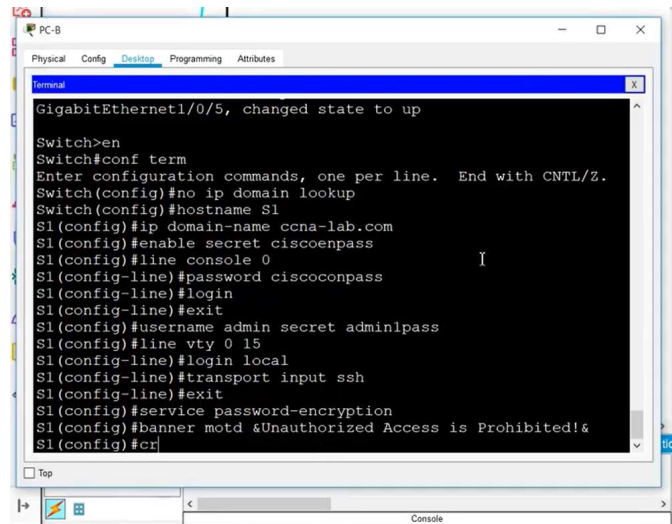
Se configuran las siguientes tareas:

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 S2(config-line)#login local S2(config- line)#exit S2(config)#line vty 5 15 S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#line vty 5 15 S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2#config t S2(config)#banner motd "Este es un sistema seguro. Solo acceso autorizado"

Tabla 13. Configuración S1 y S2

En la tabla 13, configuraremos S1, crearemos una Vlan, crearemos un tronco 802.1Q para usar la VLAN 6 nativa y luego crearemos un conjunto de puertos EtherChannel de capa 2 que usan las interfaces F0 / 1 y F0 / 2. Configuración de permisos de acceso de host para VLAN 2

Figura 15. Configuración de las tareas



```
GigabitEthernet1/0/5, changed state to up
Switch>en
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain lookup
Switch(config)#hostname S1
S1(config)#ip domain-name cca-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret adminpass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd &Unauthorized Access is Prohibited!&
S1(config)#cr
```

Fuente: Autor

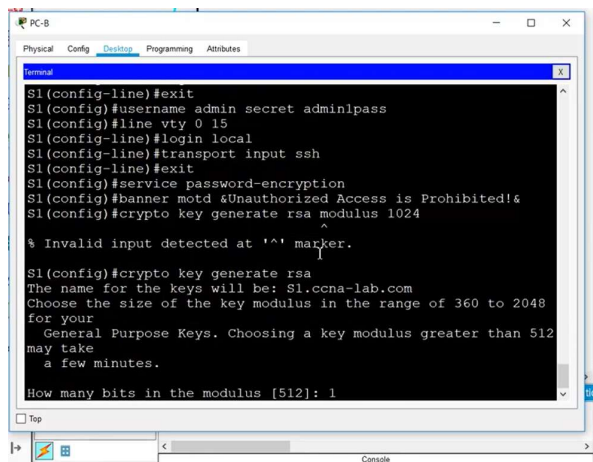
En la figura 15 se aplican las configuraciones dada por la tabla 12

Generar una clave de cifrado RSA	Módulo de 1024 bits
----------------------------------	----------------------------

Tabla 14. Clave de cifrado RSA

En la tabla 14 se muestra el Cifrado RSA donde el modulo debe ser de 1024 bits respectivamente

Figura 16. Clave de cifrado RSA



Fuente: Autor

En la figura 16 se muestra que se soporta en uno real configuramos respectivamente.

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 Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Tabla 15. Gateway predeterminado

En la tabla 15 se configura la interfaz y la Configuración del Gateway.

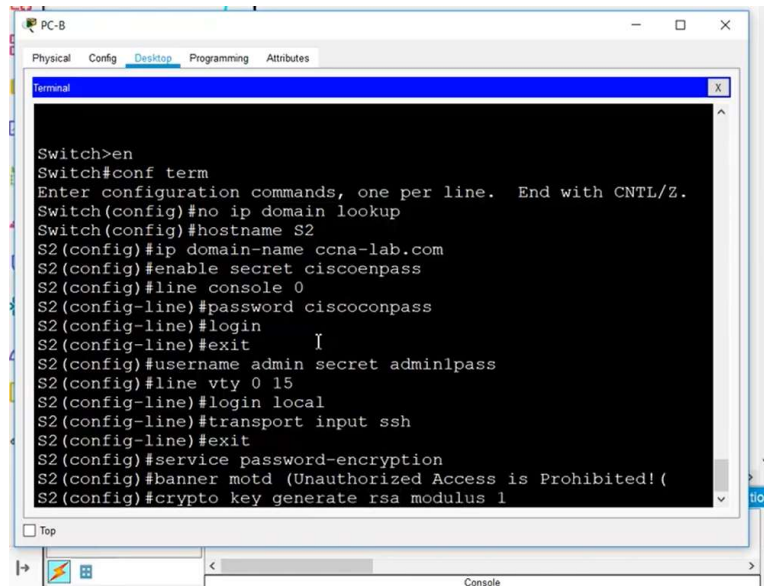
Se debe tener en cuenta la tabla de direccionamiento:

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde

Tabla 16. S1 VLAN 4

En la tabla 16 se muestra como se conecta la PC-A desde el puerto de la consola al puerto de la consola de R1 mediante un cable de consola, como en la vida real, y use el siguiente comando para eliminar la configuración inicial de R1.

Figura 17. Configuración direccionamiento



Fuente: Autor

En la figura 18 se muestra la configuración del PC-B donde s2 es configurada en los diferentes puntos de la interfaz y el dispositivo

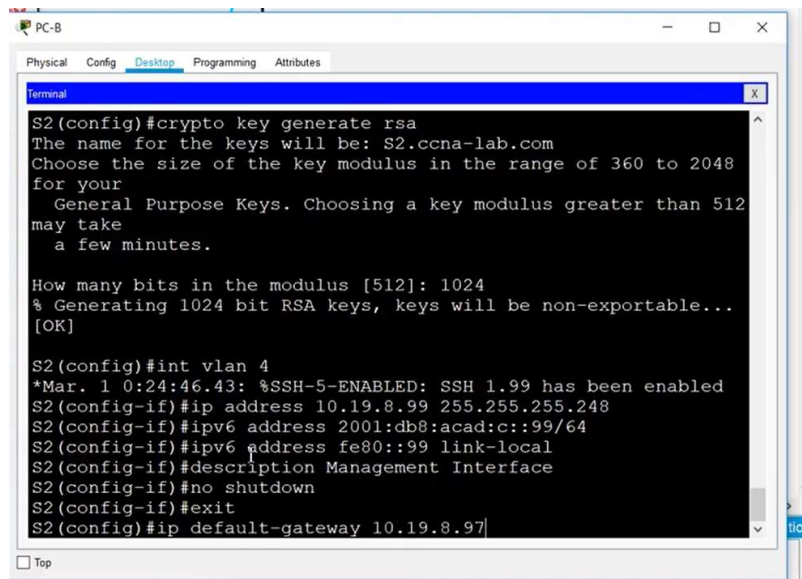
Se Utiliza la tabla

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde

Tabla 17. S2 VLAN 4

En la tabla 17 se ve la interfaz S2 VLAN 4 con sus respectivas configuraciones y la puerta de enlace predeterminada.

Figura 18. S2 VLAN 4 configurado



Fuente: Autor

En la figura 19 se aplica la configuración respectiva al S2 del VLAN 2 previamente configurado, se aplica en módulo de bit así como las direcciones.

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

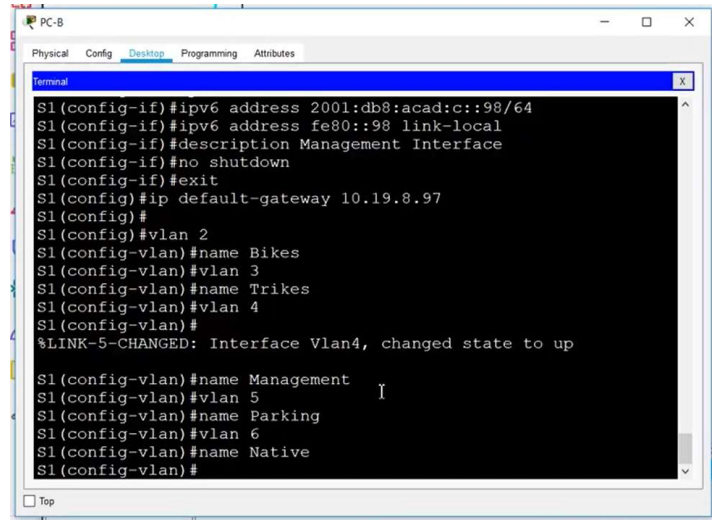
Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native

Tabla 18. Crear VLAN

En la tabla 18 se ven las VLAN las cuales se deben crear teniendo en cuenta los nombres Parking, Native, Triket, Bikes y Management.

Se crean las VLAN

Figura 19. VLAN creadas



```
PC-B
Physical Config Desktop Programming Attributes
Terminal
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
S1(config)#ip default-gateway 10.19.8.97
S1(config)#
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)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
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)#
```

Fuente: Autor

En la figura 20 Se nota configurada VLAN, Trunk y Etherchannel en los dos switches. Además, la configuración de seguridad se realiza en los puertos de acceso y las interfaces no utilizadas se agrupan en VLAN específicas.

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5

Tabla 19. Troncos 802.1Q

En la tabla 19 se muestra la tarea donde se debe crear troncos 802.1Q, es importante que usen la VLAN 6 nativa.

Figura 20. Troncos 802.1Q

```

S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#int g1/0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed
state to up

S1(config-if)#switchport trunk native vlan 6
S1(config-if)#int range g1/0/1-2
S1(config-if-range)#shutdown
    
```

Fuente: Autor

En la figura 21 se aplica la configuración de la tarea con sus respectivas interfaces finalizando el shutdown.

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación

Tabla 20. Puertos EtherChannel

Figura 21. Grupo de puertos EtherChannel

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/2, changed state to down

S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/1 is 6, Pol id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/2 is 6, Pol id 1)

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
S1(config-if)#
    
```

Fuente: Autor

En la figura 22 se Crear un grupo de puertos EtherChannel muestra la configuración

del protocolo LACP

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6

Tabla 21. Puerto de acceso de host

La tabla 21 muestra la tarea del puerto de acceso de host, la especificación requerida es la Interface F0/6

Figura 22. Grupo de puertos EtherChannel

```

PC-B
-----
Physical Config Desktop Programming Attributes
Terminal
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/1 is 6, Pol id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/2 is 6, Pol id 1)

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
S1(config-if)#int g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#
    
```

Fuente: Autor

En la figura 23 se aplica la configuración de la Vlan 2 donde la Interface F0/6 es la especificación seleccionada

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC

Tabla 22. Seguridad del puerto

La tabla 22 se especifica la configuración del puerto de los puertos de acceso donde se permiten 3 direcciones MAC

Figura 23. Puerto en los puertos de acceso

```

PC-B
Physical Config Desktop Programming Atributos
Terminal
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 1)

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
S1(config-if)#int g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#
    
```

Fuente: Autor

En la figura 24 se configuran los puertos de acceso se permiten las 3 direcciones MAC

Tarea	Especificación
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 23. Interfaces no utilizadas

La tabla 23 muestra la tarea de protección de las interfaces que no se van a utilizar en el proceso, se asigna a VLAN 5

Figura 24. Protección de interfaces

```

S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#int g1/0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#int range g1/0/3-4
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

%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state
to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state
to administratively down
S1(config-if-range)#
S1(config-if-range)#
    
```

Fuente: Autor

En la figura 25 se aplican la configuración de interfaces S1, por medio de #Switchport

Paso 5: Configure el S2.

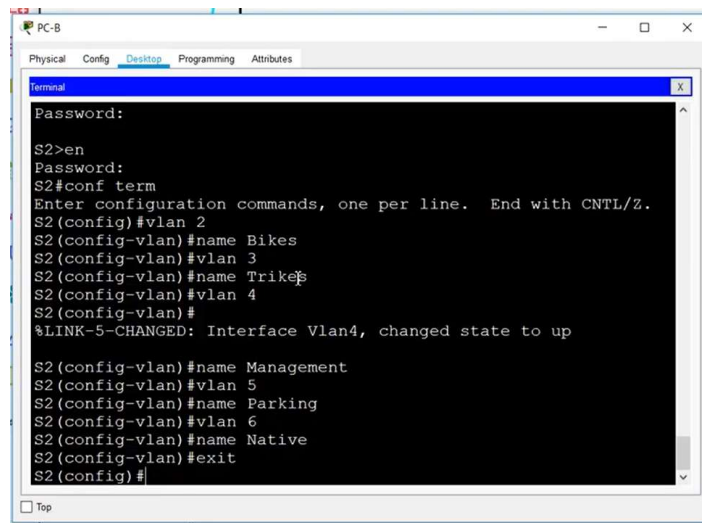
Entre las tareas de configuración de S2 se incluyen las siguientes:

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native

Tabla 24. Crear VLAN

En la tabla 24 se crean las VLAN con las especificaciones en los nombres Bikes, Trikes, Management, Parking y Native respectivamente

Figura 25. Crear VLAN



Fuente: Autor

En la figura 26 se comprueba que en PC-B se crea cada uno de los VLANS con las especificaciones solicitadas, así como los nombres que solicita la tabla.

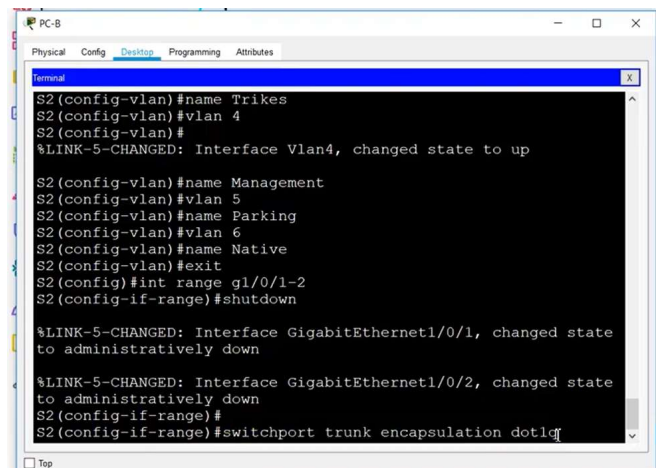
Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2

Tabla 25. VLAN 6 nativa

La tabla 25 especifica la tarea en la que se debe crear troncos 802.1Q respondiendo a las especificaciones de Interfaces F0/1 y F0/2

Se crean troncos 802.1Q que utilizan la VLAN 6 nativa

Figura 26. Troncos 802.1Q



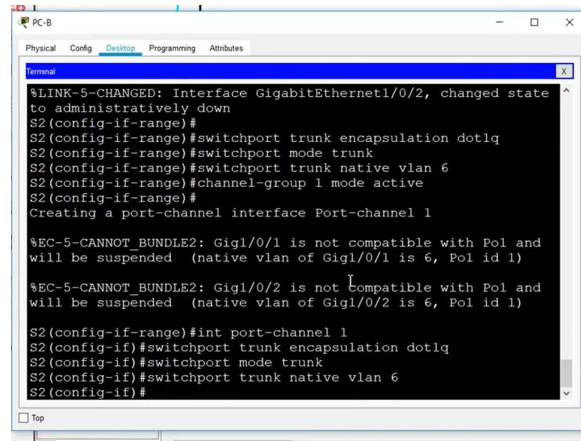
```
PC-B
Physical Config Desktop Programming Attributes
Terminal
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#int range g1/0/1-2
S2(config-if-range)#shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state
to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state
to administratively down
S2(config-if-range)#
S2(config-if-range)#switchport trunk encapsulation dot1q
```

Fuente: Autor

En la figura 27 es aplicada las Interfaces F0/1 y F0/2 en los Troncos 802.1Q

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, se usan el protocolo LACP para la negociación

Figura 27. Puertos EtherChannel de Capa 2



```
PC-B
Physical Config Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state
to administratively down
S2(config-if-range)#
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1
%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1)
%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 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
S2(config-if)#
```

Fuente: Autor

En la figura 28 se configura el puerto de acceso del host para la VLAN 3, interfaz F0/18

Figura 28. Puerto de acceso del host

```

PC-8
Physical Config Desktop Programming Attributes
Terminal
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 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
S2(config-if)#int g1/0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#
    
```

Fuente: Autor

En la figura 29 se hace el Puerto de acceso del host

Configure port-security en los access ports	permite 3 MAC addresses
---	-------------------------

Tabla 26. Port-security en los Access

En la tabla 26 se solicita la configuración los puerto de acceso en la cual se permiten 3 direcciones de MAC

Figura 29. Port-security en los access ports

```

PC-8
Physical Config Desktop Programming Attributes
Terminal
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/1 is 6, Po1 id 1)

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and
will be suspended (native vlan of Gig1/0/2 is 6, Po1 id 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
S2(config-if)#int g1/0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#
    
```

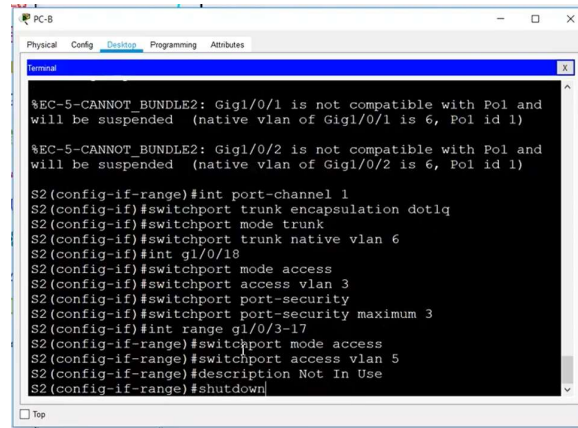
Fuente: Autor

En la figura 30 se aplica port-security maximum 3 en el cual solo se aceptan las tres direcciones MAC.

Se aseguran todas las interfaces no utilizadas, VLAN 5, se establece modo de

acceso, agregar una descripción y apagar

Figura 30. Interfaces no utilizadas



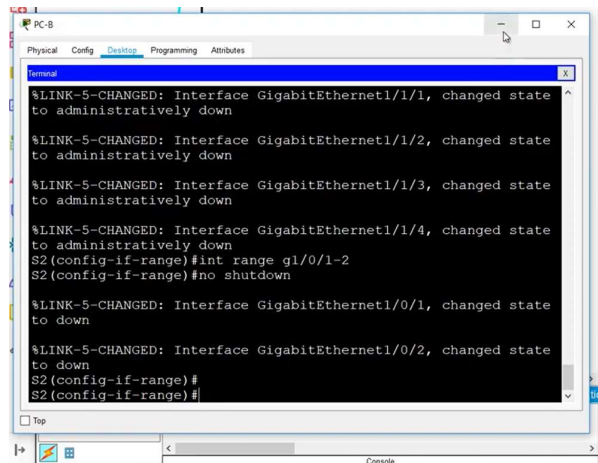
```
PC-B
Physical Config Desktop Programming Attributes
Terminal
%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/1 is 6, Pol id 1)
%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Pol and
will be suspended (native vlan of Gig1/0/2 is 6, Pol id 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
S2(config-if)#int g1/0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#int range g1/0/3-17
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
```

Fuente: Autor

En la figura 31 se establecen el modo de acceso, agregar una descripción y apagar.

Se activan:

Figura 31. Activación



```
PC-B
Physical Config Desktop Programming Attributes
Terminal
%LINK-5-CHANGED: Interface GigabitEthernet1/1/1, changed state
to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/2, changed state
to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/3, changed state
to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet1/1/4, changed state
to administratively down
S2(config-if-range)#int range g1/0/1-2
S2(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state
to down
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state
to down
S2(config-if-range)#
S2(config-if-range)#
```

Fuente: Autor

En la figura 32 se muestra la activación dentro del PC-B

Parte 2: Configurar soporte de host

Paso 1: Configure R1

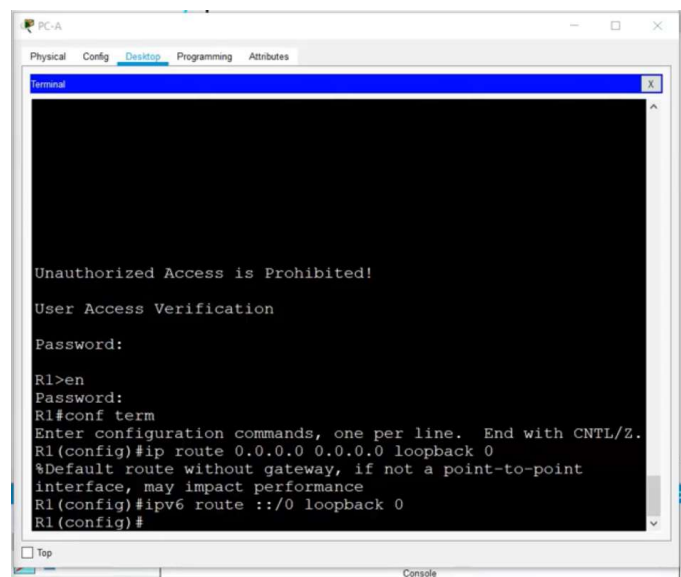
Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

Tabla 27. Configure Default Routing

En la tabla 27 se especifica la tarea de configuración del routing por defecto con las rutas Ipv4 e Ipv6

Figura 32. Configuración Default Routing



Fuente: Autor

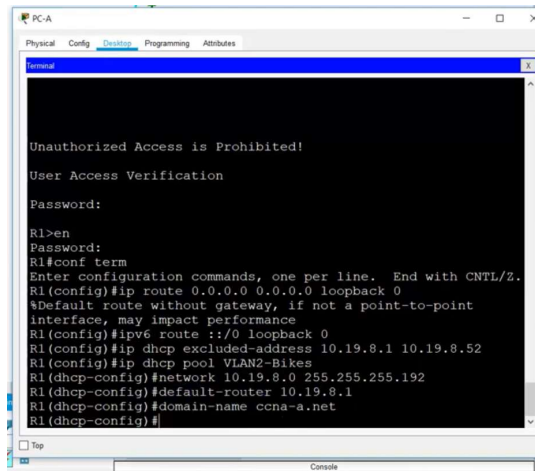
En la figura 33 se configura desde el PC-A en la configuración del routing por defecto con las rutas Ipv4 e Ipv6

Tarea	Especificación
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Tabla 28. IPv4 DHCP para VLAN 2

La tabla 28 muestra la configuración que se debe hacer al IPv4 DHCP para VLAN

Figura 33. IPv4 DHCP para VLAN 2



Fuente: Autor

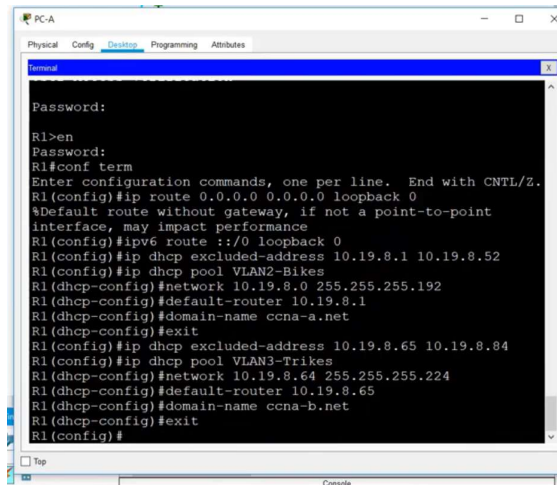
En la figura 34 vemos la ejecución del grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Tabla 29. DHCP IPv4 para VLAN 3

En la tabla 29 se muestra la tarea respectiva a la DHCP IPv4 para VLAN 3 con las respectivas asignaciones.

Figura 34. DHCP IPv4 para VLAN 3



```
PC-A
Physical Config Desktop Programming Attributes
Terminal
Password:
R1>en
Password:
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#ip route ::/0 loopback 0
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
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
R1(config)#
```

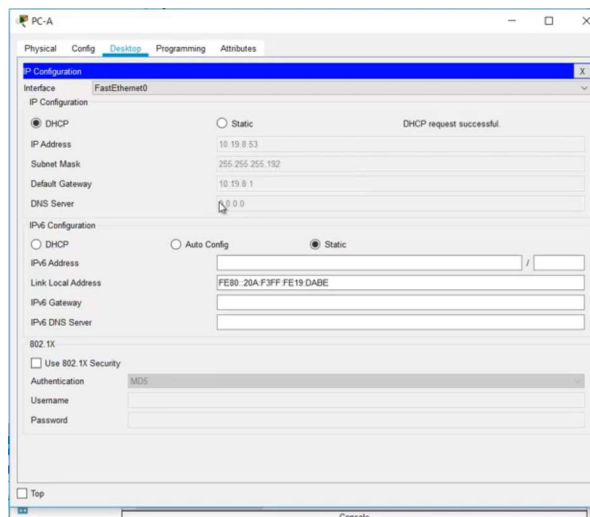
Fuente: Autor

En la figura 35 se muestra la ejecución del DHCP IPv4 para VLAN 3

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**.

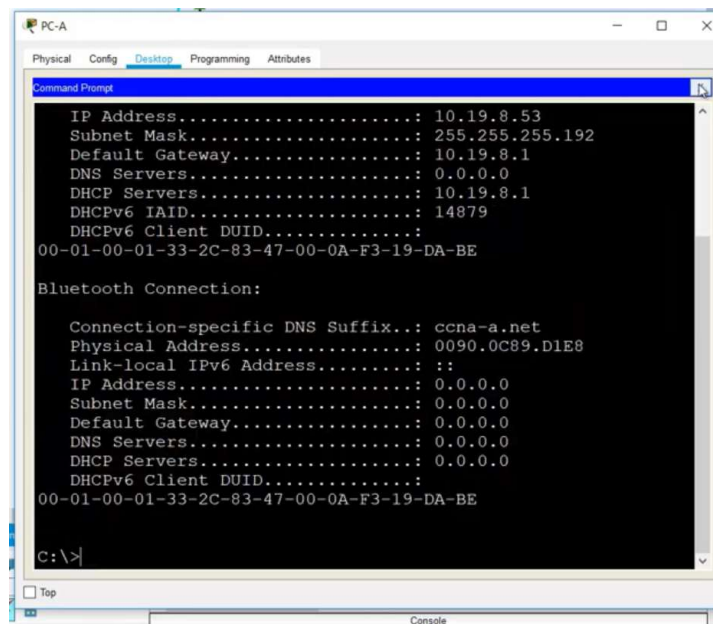
Figura 35. Host PC-A y PC-B



Fuente: Autor

La figura 36 muestra el registro de las configuraciones de red del host con el comando **ipconfig /all**

Figura 36. PC-A y PC-B



Fuente: Autor

La figura 37 muestra las conexiones PC-A y PC-B con las configuraciones host para que utilicen DHCP

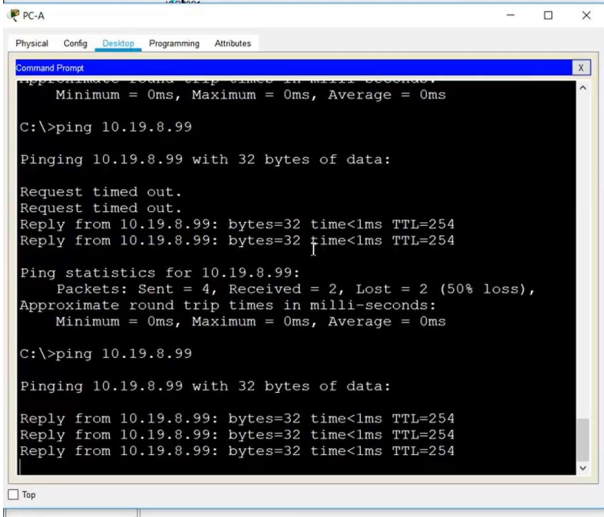
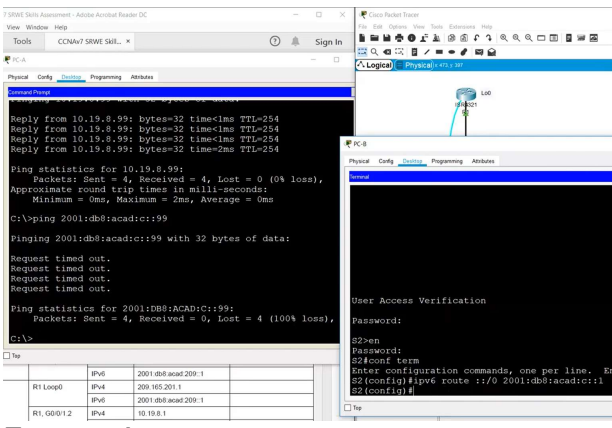
Parte 3: extremo

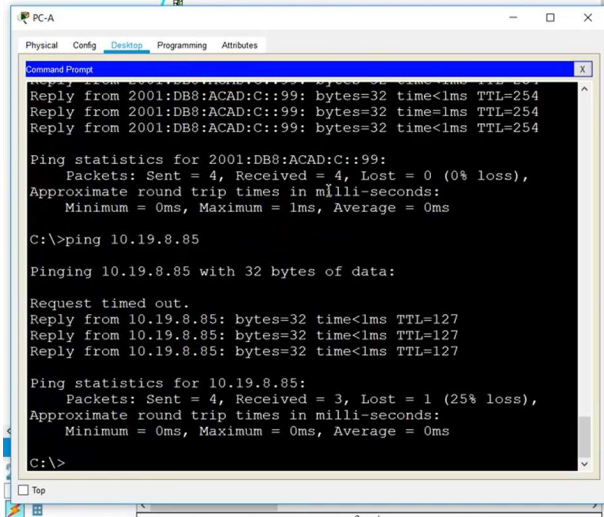
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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:

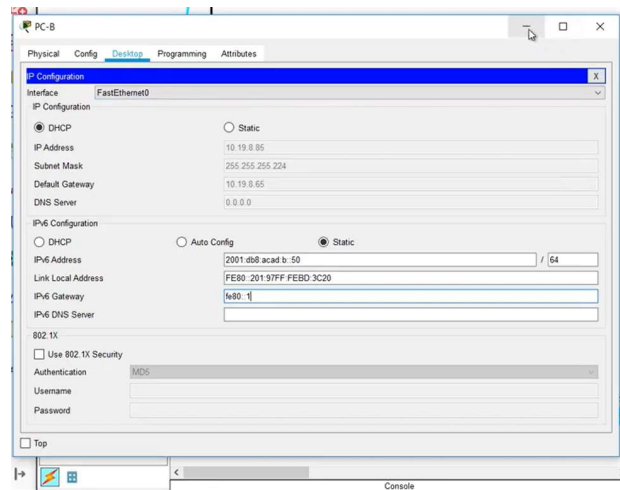
A continuación, se evidencian los resultados del Ping con la respectiva dirección IP demostrando la funcionalidad de las configuraciones en el Packet tracer

Dirección IP	Resultados de ping
10.19.8.99.	<p>Figura 37. 10.19.8.99.</p>  <pre> C:\>ping 10.19.8.99 Pinging 10.19.8.99 with 32 bytes of data: Request timed out. Request timed out. Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Ping statistics for 10.19.8.99: Packets: Sent = 4, Received = 2, Lost = 2 (50% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 10.19.8.99 Pinging 10.19.8.99 with 32 bytes of data: Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 </pre> <p>Fuente: Autor</p>
2001:db8:acad:c: :99	<p>Figura 38. 10.19.8.99.</p>  <pre> C:\>ping 10.19.8.99 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<2ms TTL=254 Ping statistics for 10.19.8.99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms C:\>ping 2001:db8:acad:c::99 Pinging 2001:db8:acad:c::99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:db8:acad:c::99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), </pre> <p>Fuente: Autor</p>

Dirección IP	Resultados de ping
<p>IP address will vary.</p>	<p>Figura 39. IP address will vary.</p>  <pre> C:\>ping 2001:DB8:ACAD:C::99 Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time=1ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\>ping 10.19.8.85 Pinging 10.19.8.85 with 32 bytes of data: Request timed out. Reply from 10.19.8.85: bytes=32 time<1ms TTL=127 Reply from 10.19.8.85: bytes=32 time<1ms TTL=127 Reply from 10.19.8.85: bytes=32 time<1ms TTL=127 Ping statistics for 10.19.8.85: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p>Fuente: Autor</p>

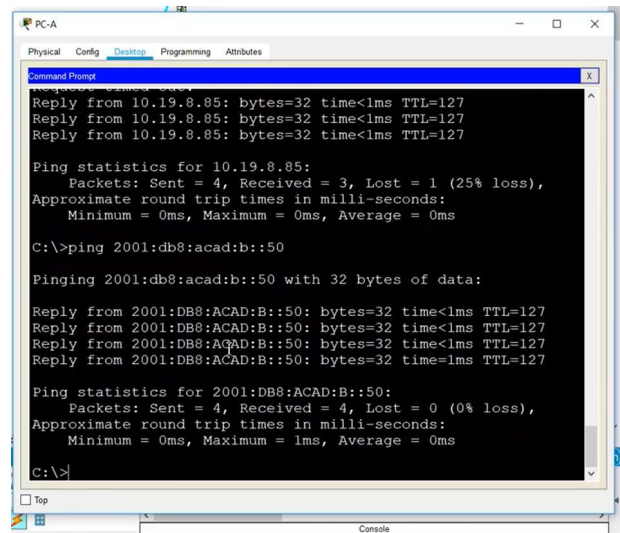
Dirección IP	Resultados de ping
--------------	--------------------

Figura 40. 2001:db8:acad:b::50



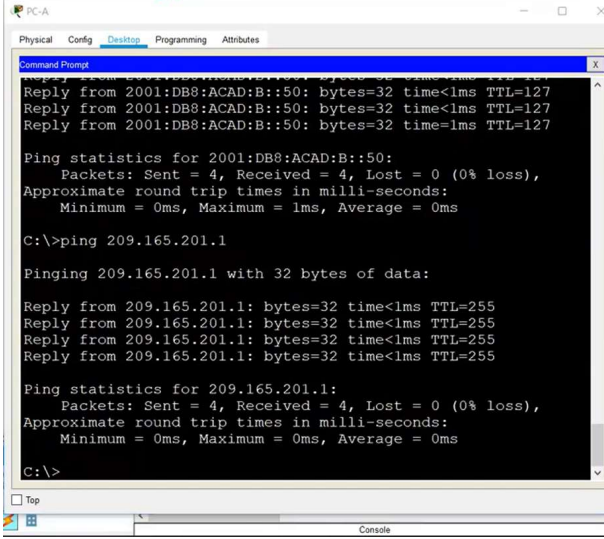
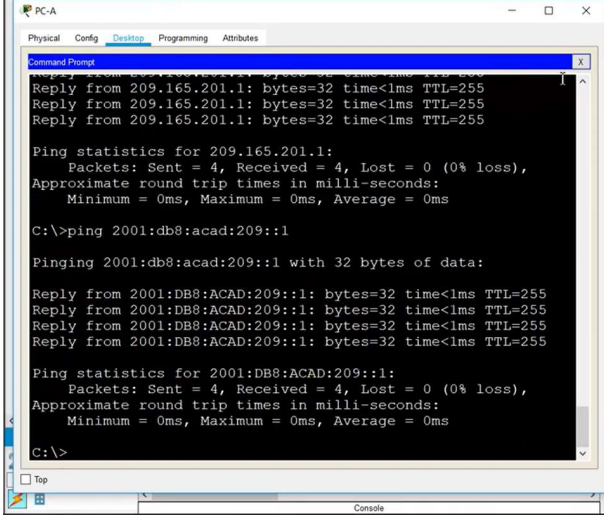
Fuente: Autor

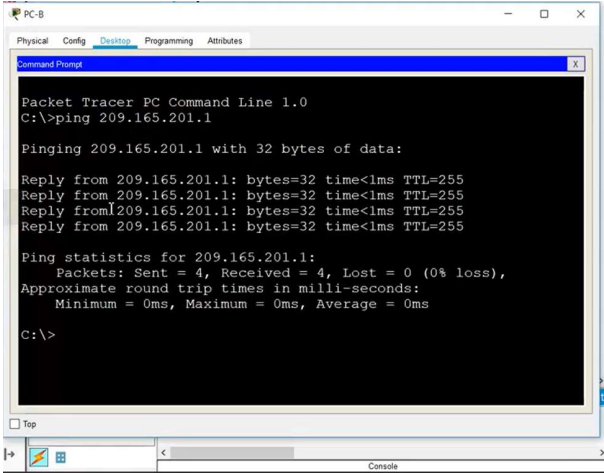
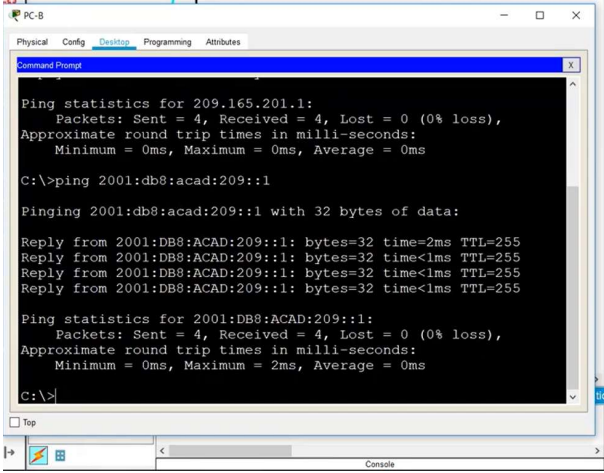
Figura 41. 2001:db8:acad:b::50

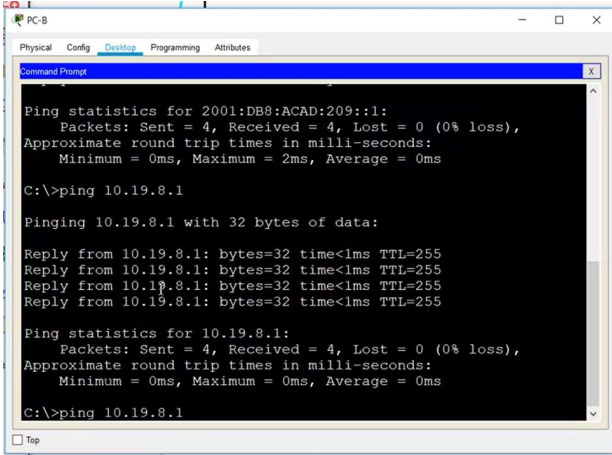
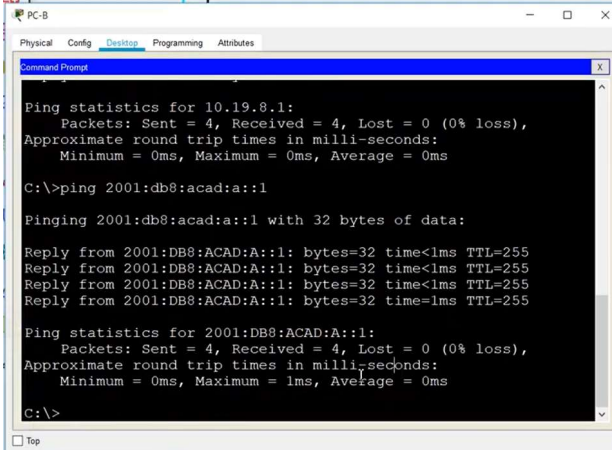


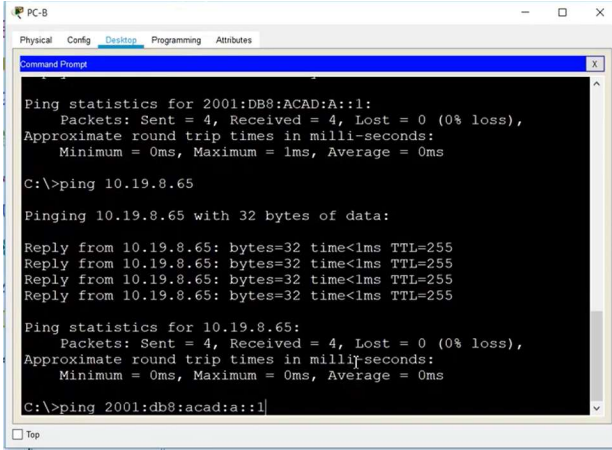
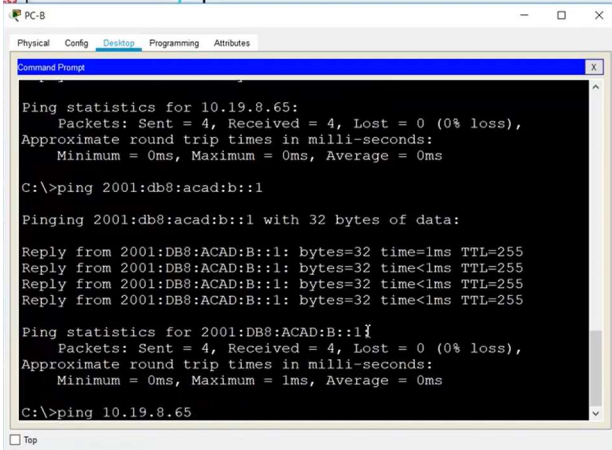
Fuente: Autor

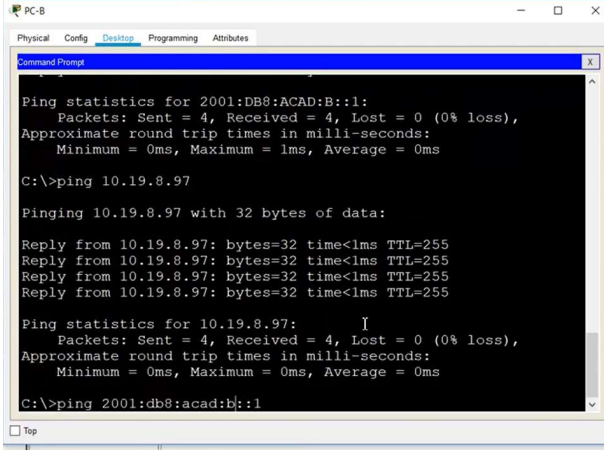
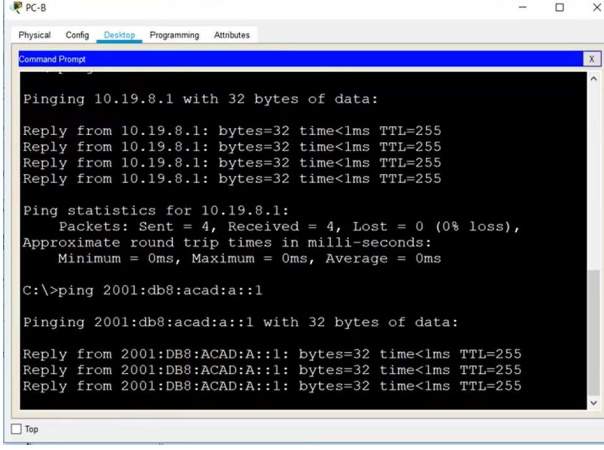
2001:db8:acad:b:
:50

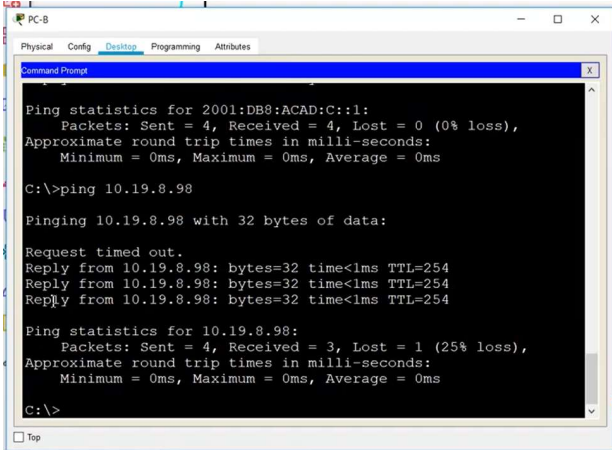
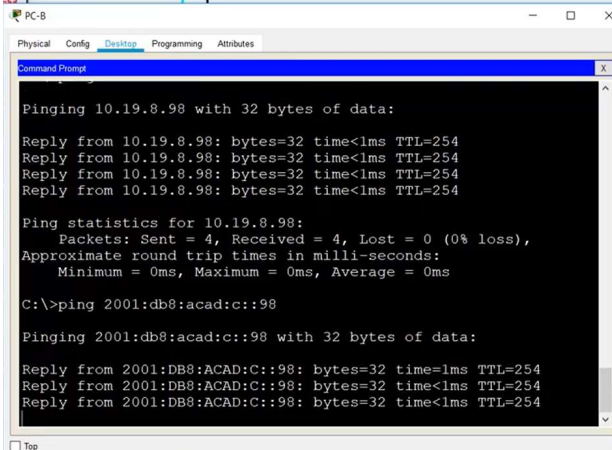
Dirección IP	Resultados de ping
209.165.201.1	<p>Figura 42. 209.165.201.1</p>  <pre> C:\>ping 209.165.201.1 Pinging 209.165.201.1 with 32 bytes of data: Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p>Fuente: Autor</p>
2001:db8:acad:209::1	<p>Figura 43. 2001:db8:acad:209::1</p>  <pre> C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p>Fuente: Autor</p>

Dirección IP	Resultados de ping
209.165.201.1	<p data-bbox="646 398 997 432">Figura 44. 209.165.201.1</p>  <p data-bbox="646 929 837 963">Fuente: Autor</p>
2001:db8:acad:209::1	<p data-bbox="646 1032 1109 1066">Figura 45. 2001:db8:acad:209::1</p>  <p data-bbox="646 1563 837 1597">Fuente: Autor</p>

Dirección IP	Resultados de ping
10.19.8.1	<p data-bbox="646 398 925 432">Figura 46. 10.19.8.1</p>  <pre data-bbox="662 555 1244 873"> C:\>ping 10.19.8.1 Pinging 10.19.8.1 with 32 bytes of data: Reply from 10.19.8.1: bytes=32 time<1ms TTL=255 Reply from 10.19.8.1: bytes=32 time<1ms TTL=255 Reply from 10.19.8.1: bytes=32 time<1ms TTL=255 Reply from 10.19.8.1: bytes=32 time<1ms TTL=255 Ping statistics for 10.19.8.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 10.19.8.1 </pre> <p data-bbox="646 918 837 952">Fuente: Autor</p>
2001:db8:acad:a: :1	<p data-bbox="646 1025 1069 1059">Figura 47. 2001:db8:acad:a: :1</p>  <pre data-bbox="662 1182 1244 1500"> C:\>ping 2001:db8:acad:a::1 Pinging 2001:db8:acad:a::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms C:\> </pre> <p data-bbox="646 1534 837 1568">Fuente: Autor</p>

Dirección IP	Resultados de ping
10.19.8.65	<p data-bbox="646 398 948 432">Figura 48. 10.19.8.65</p>  <p data-bbox="646 909 839 943">Fuente: Autor</p>
2001:db8:acad:b: :1	<p data-bbox="646 1014 1075 1048">Figura 49. 2001:db8:acad:b: :1</p>  <p data-bbox="646 1525 839 1559">Fuente: Autor</p>

Dirección IP	Resultados de ping
10.19.8.97	<p data-bbox="646 398 949 432">Figura 50. 10.19.8.97</p>  <p data-bbox="646 913 837 947">Fuente: Autor</p>
2001:db8:acad:c::1	<p data-bbox="646 1016 1077 1050">Figura 51. 2001:db8:acad:c::1</p>  <p data-bbox="646 1532 837 1565">Fuente: Autor</p>

Dirección IP	Resultados de ping
10.19.8.98	<p data-bbox="646 398 948 432">Figura 52. 10.19.8.98</p>  <pre data-bbox="662 555 1173 880"> C:\>ping 10.19.8.98 Pinging 10.19.8.98 with 32 bytes of data: Request timed out. Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Ping statistics for 10.19.8.98: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p data-bbox="646 909 837 943">Fuente: Autor</p>
2001:db8:acad:c: :98	<p data-bbox="646 1014 1091 1048">Figura 53. 2001:db8:acad:c: :98</p>  <pre data-bbox="662 1171 1189 1496"> C:\>ping 10.19.8.98 Pinging 10.19.8.98 with 32 bytes of data: Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Reply from 10.19.8.98: bytes=32 time<lms TTL=254 Ping statistics for 10.19.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 2001:db8:acad:c::98 Pinging 2001:db8:acad:c::98 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::98: bytes=32 time=lms TTL=254 Reply from 2001:DB8:ACAD:C::98: bytes=32 time<lms TTL=254 Reply from 2001:DB8:ACAD:C::98: bytes=32 time<lms TTL=254 </pre> <p data-bbox="646 1525 837 1559">Fuente: Autor</p>

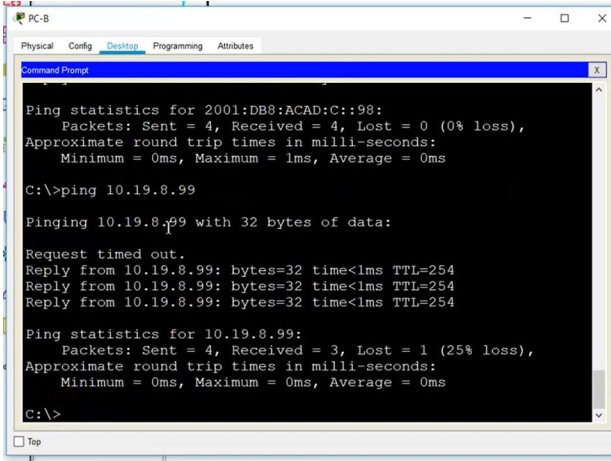
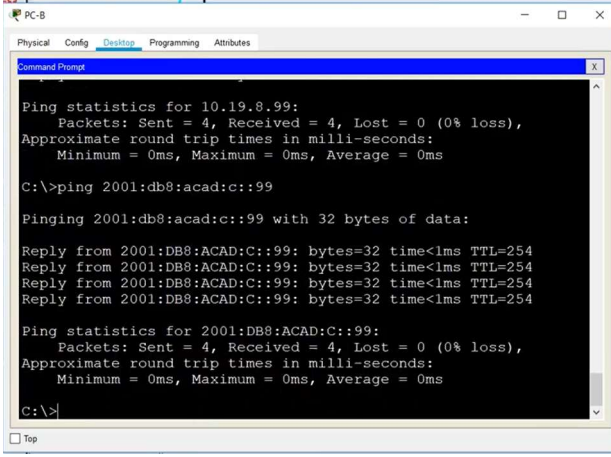
Dirección IP	Resultados de ping
<p>10.19.8.99.</p>	<p>Figura 54. 10.19.8.99.</p>  <pre> C:\>ping 10.19.8.99 Pinging 10.19.8.99 with 32 bytes of data: Request timed out. Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Ping statistics for 10.19.8.99: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p>Fuente: Autor</p>
<p>2001:db8:acad:c: :99</p>	<p>Figura 55. 2001:db8:acad:c: :99</p>  <pre> C:\>ping 2001:db8:acad:c::99 Pinging 2001:db8:acad:c::99 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254 Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\> </pre> <p>Fuente: Autor</p>

Tabla 30. Ejecución de pruebas ping

En la tabla 30 se evidencia la ejecución correcta de las diferentes direcciones y pruebas del ping

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

Tabla 31. Pruebas ping

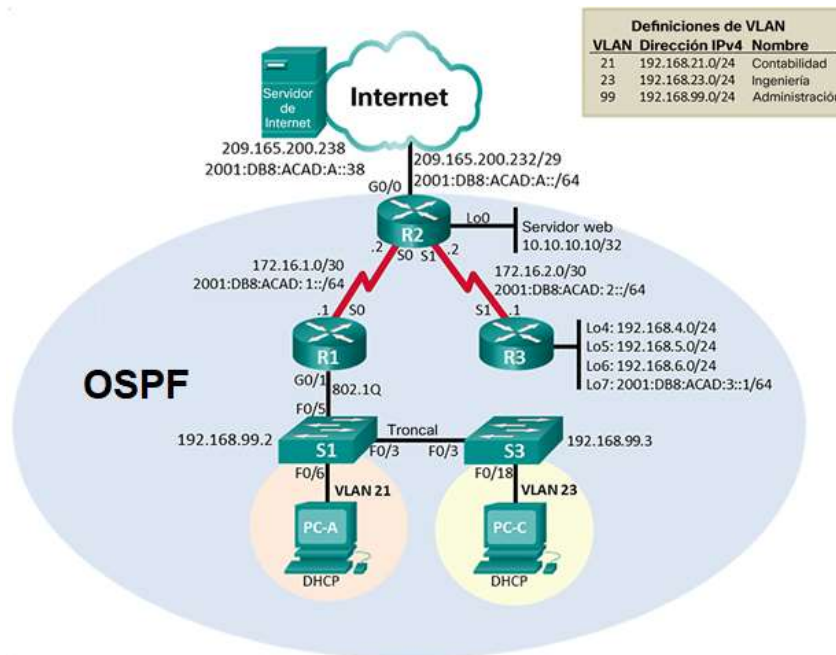
La tabla 31 muestra los resultados del ping en concreto y evidencia las únicas dos fallas presentadas.

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) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología

Figura 56: Topología escenario 2

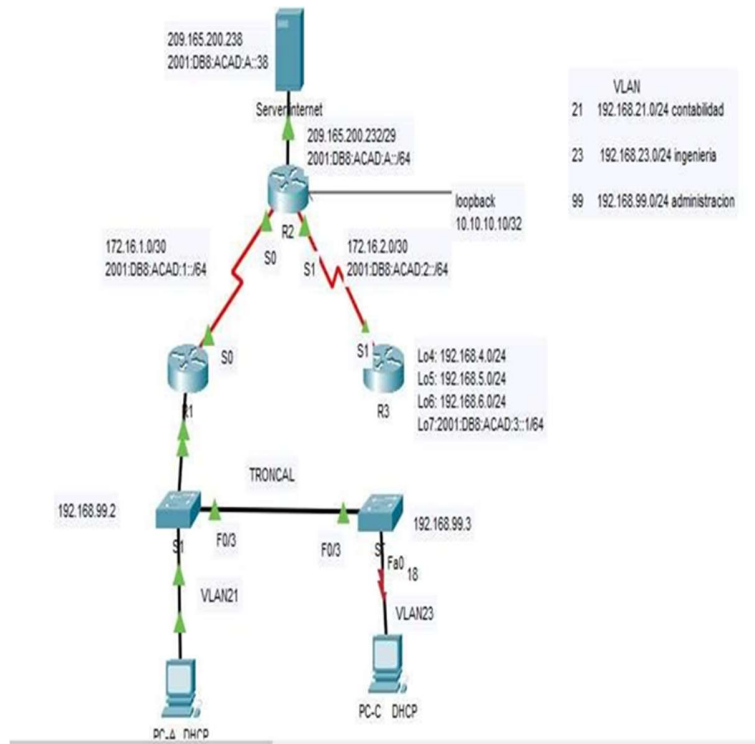


Fuente: Documento del Repositorio

La figura 57 muestra la topología a desarrollar dentro del escenario

Parte 1: Inicializar dispositivos

Figura 57: Topología del escenario



Fuente: Autor

En la figura 59 se realiza la topología del escenario dentro del Software

Paso 1: Inicializar y volver a cargar los routers 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.

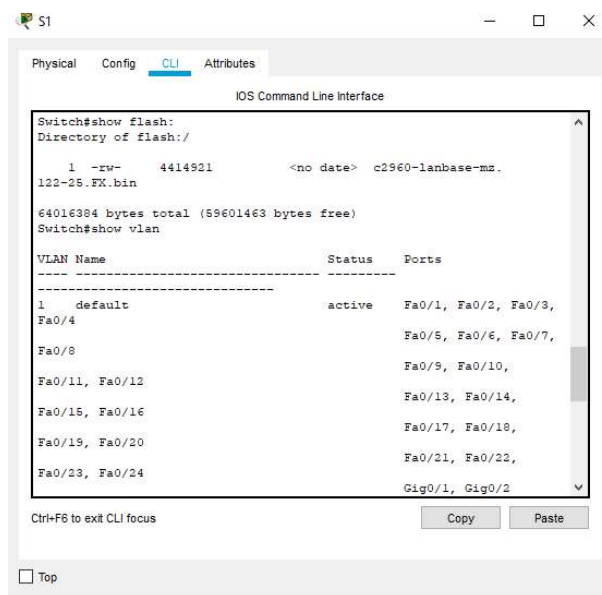
Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Ejecutamos el siguiente código: Erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	#erase startup-config

Volver a cargar ambos switches	Ejecutamos: no shutdown
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash: Switch#show vlan

Tabla 32. Comando de inicializar dispositivos

En la tabla 32 se especifican las diferentes tareas de configuración con los comando de IOS

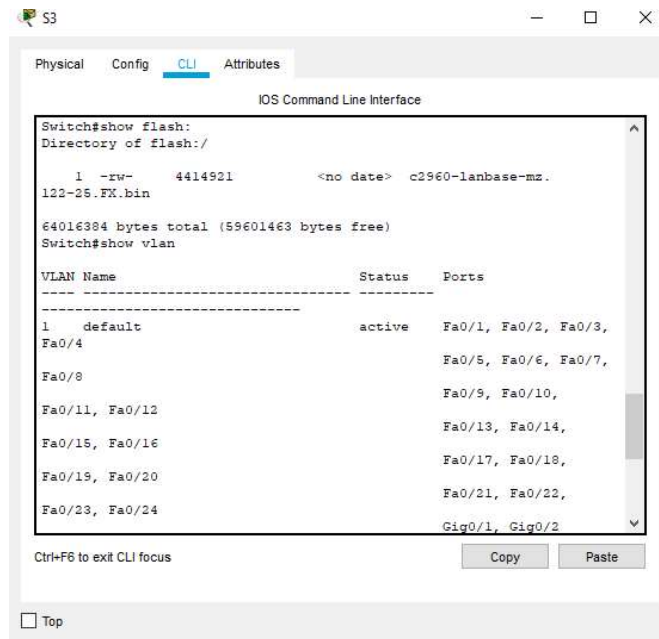
Figura 58. Tarea Comando de IOS



Fuente: Autor

En la figura 60 se evidencia la aplicación de la tarea de comandos IOS Command Line interface evidenciando funcionamiento. Se verifica que la base de datos de VLAN está en la memoria flash en ambos switches.

Figura 59. Ejecución no shutdown



Fuente: Autor

En la figura 61 se muestra la ejecución de los VLANS

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 2: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 33. Tarea de configuración

En la tabla 33 se muestra las tarea de configuración y las respectivas especificaciones.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	hostname R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	Se ingresa el código: line con 0 password cisco
Contraseña de acceso Telnet	Se ingresa el código: line vty 0 4 password Cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	#Se prohíbe el acceso no autorizado!#
Interfaz S0/0/0	R1(config)#interface s0/0/0 Establezca la descripción: R1(config-if)#description Conexion a R2 Establecer la dirección IPv4: R1(config-if)#ip add 172.16.1.1 255.255.255.252 Establecer la dirección IPv6: R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64 Establecer la frecuencia de reloj en 128000: R1(config-if)#clock rate 128000 Activar la interfaz: R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ipv6 unicast-routing Configurar una ruta IPv4 predeterminada de S0/0/0: R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0: R1(config)#ipv6 route ::/0 s0/0/0

Tabla 34. Tarea de configuración

En la tabla 34 se muestran las tareas de configuración de R1

```
R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-
line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #Se prohíbe el acceso no autorizado!# R1
(config)#ipv6 unicast-routing
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ip v
address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000
R1(config-if)#description R1-R2 R1(config-if)#no shutdown R1
(config)#ipv6 route ::/0 serial 0/0/0
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

Tabla 35. R1 Config

En la tabla R1 se constata el resultado de R1 con las configuraciones aplicadas

Nota: Todavía no configure G0/1.

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	line con 0 password Cisco
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config- line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	#Service password-encryption

Habilitar el servidor HTTP	<pre>ip nat inside source static 10.10.10.10 209.165.200.229 int f0/0 ip nat outside int f0/1 ip nat inside</pre>
Mensaje MOTD	<pre>banner motd! ¡Se prohíbe el acceso no autorizado!</pre>
Interfaz S0/0/0	<pre>Establezca la descripción R2-R1 Establezca la dirección IPv4 Utilizar la siguiente dirección disponible en la subred. 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. 2001:DB8:ACAD:1::1/64 Activar la interfaz</pre>
Interfaz S0/0/1	<pre>Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int s0/0/1 ip address 172.16.2.1 255.255.255.0 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. ipv6 address 2001:DB8:ACAD:3::/64 Establecer la frecuencia de reloj en 128000. clock rate 128000 Activar la interfaz</pre>
Interfaz G0/0 (simulación de Internet)	<pre>R2(config)#int g0/0 Establecer la descripción: R2(config-if)#description Conexion a Internet Establezca la dirección IPv4: R2(config-if)#ip add 209.165.200.233 255.255.255.248 Establezca la dirección IPv6: R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 Activar la interfaz: R2(config-if)#no shutdown</pre>
Interfaz loopback 0 (servidor web simulado)	<pre>Establecer la descripción.R2-web server Establezca la dirección IPv4. 10.10.10.1 255.255.255.0</pre>

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.
---------------------	--

Tabla 36. Configuración R2

En la tabla 36 se configura R2 con las tareas de configuración

Figura 60. Configuración del R2

```

R2
-----
Physical  Config  CLI  Attributes
-----
IOS Command Line Interface

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#banner motd %U
R2(config)#banner motd %Unauthorized Access is prohibited%
R2(config)#int s0/0/0
R2(config-if)#description Connection to R1

% Invalid input detected at '^' marker.

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 200::db8:acad:1::2/64
R2(config-if)#no shu

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#

```

Fuente: Autor

En la figura 62 se muestra la configuración del R2

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-look
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	class

Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	line vty 0 password Cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	#Se prohíbe el acceso no autorizado!#
Interfaz S0/0/1	<p>Establecer la descripción interface serial 0/0/0 description 1</p> <p>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred: 172.16.2.0/30</p> <pre>int s0/0/1 ip address 172.16.2.6 255.255.255.252</pre> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. 2001:DB8:ACAD:2::/64</p> <pre>ipv6 address 2001:DB8:ACAD:2::/64</pre> <p>Activar la interfaz</p>
Interfaz loopback 4	<pre>R3(config)#int loopback4</pre> <p>Establezca la dirección IPv4:</p> <pre>R3(config-if)#ip add 192.168.4.1 255.255.255.0</pre>
Interfaz loopback 5	<p>Establezca la dirección IPv4. 192.168.5.1 255.255.255.0 Utilizar la primera dirección disponible en la subred.</p>
Interfaz loopback 6	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>int lo6 ip address 192.168.6.2 255.255.255.0</pre>
Interfaz loopback 7	<pre>R3(config)#int loopback7</pre> <p>Establezca la dirección IPv6:</p> <pre>R3(config-if)#ipv6 add 2001:DB8:ACAD:3::1/64</pre>
Rutas predeterminadas	<pre>ip route 0.0.0.0.0.0.0.0 s0/0/1</pre>

Tabla 37. Configuración R3

La tabla 37 muestra la configuración que se debe aplicar a R3

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-look up
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	line con 0 password Cisco
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	#service password-encryption
Mensaje MOTD	#Se prohíbe el acceso no autorizado#

Tabla 38. Configuración R1

La tabla 38 muestra la configuración a aplicar a R1

Paso 7: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	#enable secret class
Contraseña de acceso a la consola	line con 0 password Cisco
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	#service password-encryption

Mensaje MOTD	#Se prohíbe el acceso no autorizado#
--------------	--------------------------------------

Tabla 39. Configuración S3

La tabla 39 muestra las configuraciones a aplicar a S3

Paso 8: Verificar la conectividad de la red

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

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:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.1	Successful
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Successful
PC de Internet	Gateway predeterminado	209.165.200.225	Successful

Tabla 40. Conectividad de la red

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 61. Conectividad de la red

```

R1
Physical Config CLI Attributes
IOS Command Line Interface

Se prohíbe el acceso no autorizado
User Access Verification
Password:

R1>ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/20/96 ms

R1>ping 2001:db8:acad:1::2

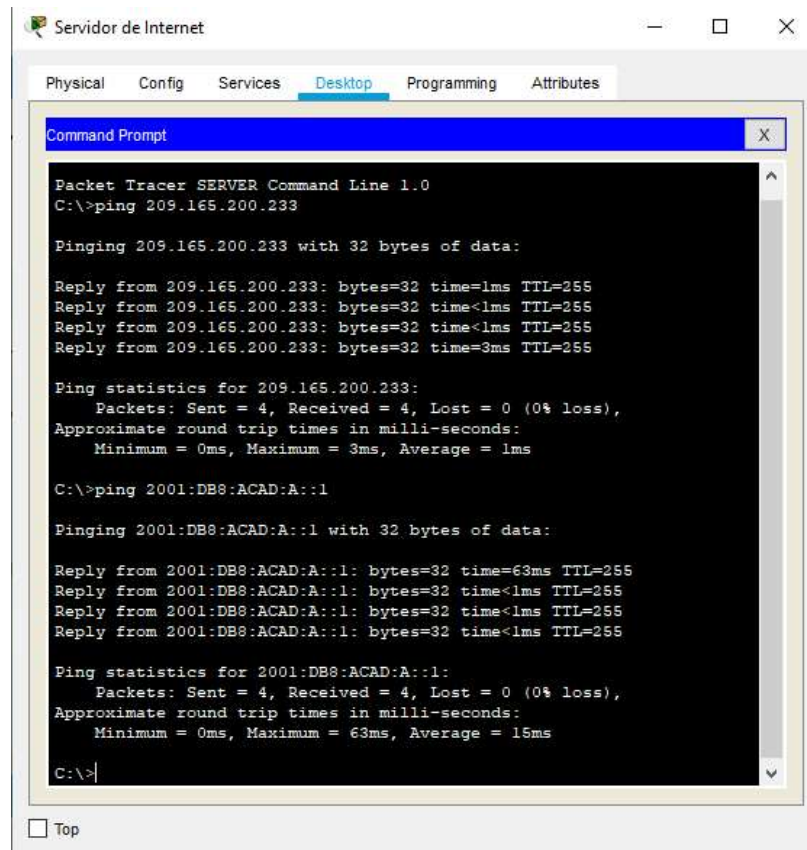
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms

R1>
  
```

Fuente: Autor

La figura 63 muestra la conectividad respectiva, se visualiza que se deshabilitó el firewall de las computadoras

Figura 62. Conectividad de la red aplicada



Fuente: Autor

La figura 64 aplica la conectividad aplicada en los diferentes servidores

Parte 2: **Configurar la seguridad del switch, las VLAN y el routing entre VLAN**

Paso 1: **Configurar S1**

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	vlan 21 name Contabilidad vlan 23 name Ingeniería vlan 99 name Administracion
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología: S1(config)#int vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa: int f0/3 switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native: S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	interface f0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Tabla 41. Configuración S1 y Routing

La tabla 41 muestra la configuración a aplicar en S1 y el routing

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN: vlan 21 name Contabilidad vlan 23 name Ingeniería vlan 99 name Administracion
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología: S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native int f0/3 switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range: S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	Utilizar el comando interface range: S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#switchport mode access
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Tabla 42. Configuración del S3

En la tabla 42 se muestran las configuraciones a aplicar en S3

Figura 63. Configurar el S3



Fuente: Autor

En la figura 65 se muestra la aplicación de las tareas y configuración en S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

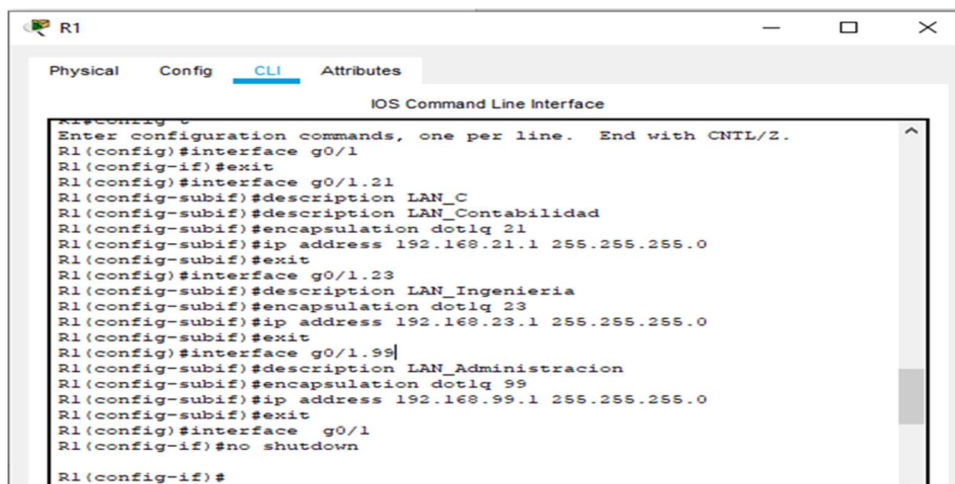
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Descripción: LAN de Contabilidad Asignar la VLAN 21</p> <p>Ingresamos: int g0/1.1 description LAN de Contabilidad encapsulation dot1Q 21</p> <p>Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 21 ip address 192.168.21.4 255.255.255.0</p>

<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p>	<p>R1(config)#int g0/1.23 Descripción: LAN de Ingeniería: R1(config-subif)#description LAN de Ingenieria Asignar la VLAN 23: R1(config-subif)#encapsulation dot1Q 23 Asignar la primera dirección disponible a esta interfaz: R1(config-subif)#ip add 192.168.23.1 255.255.255.0</p>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<p>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</p>
<p>Activar la interfaz G0/1</p>	<p>No shutdown</p>

Tabla 43. Configurar R1

En la tabla 43 se muestra la configuración a aplicar en R1

Figura 64. Configurar R1



```

R1
  Physical  Config  CLI  Attributes
  IOS Command Line Interface
  R1#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  R1(config)#interface g0/1
  R1(config-if)#exit
  R1(config)#interface g0/1.21
  R1(config-subif)#description LAN_C
  R1(config-subif)#description LAN_Contabilidad
  R1(config-subif)#encapsulation dot1q 21
  R1(config-subif)#ip address 192.168.21.1 255.255.255.0
  R1(config-subif)#exit
  R1(config)#interface g0/1.23
  R1(config-subif)#description LAN_Ingenieria
  R1(config-subif)#encapsulation dot1q 23
  R1(config-subif)#ip address 192.168.23.1 255.255.255.0
  R1(config-subif)#exit
  R1(config)#interface g0/1.99
  R1(config-subif)#description LAN_Administracion
  R1(config-subif)#encapsulation dot1q 99
  R1(config-subif)#ip address 192.168.99.1 255.255.255.0
  R1(config-subif)#exit
  R1(config)#interface g0/1
  R1(config-if)#no shutdown
  R1(config-if)#
  
```

Fuente: Autor

En la figura 66 se muestra la configuración aplicada en R1 con las interfaz G0/ y subinterfaz

Paso 4: Verificar la conectividad de la red

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

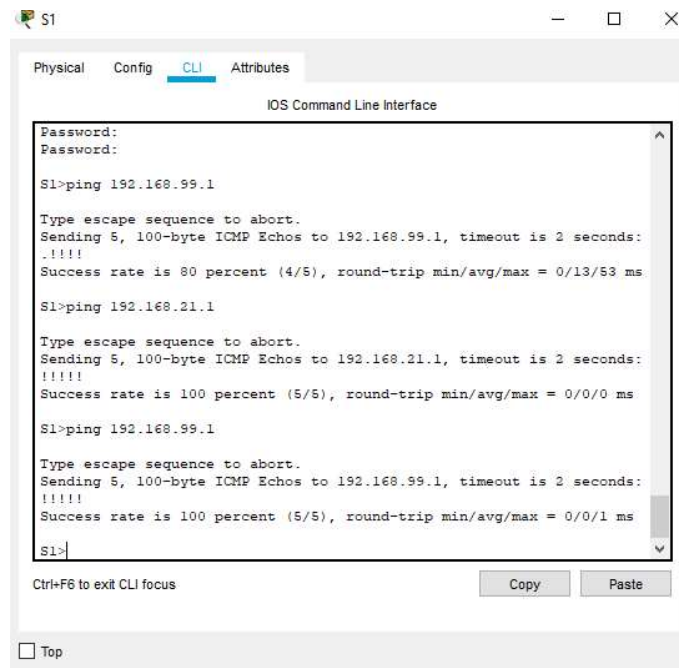
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	Successful
S3	R1, dirección VLAN 99	192.168.99.1	Successful
S1	R1, dirección VLAN 21	192.168.99.1	Successful
S3	R1, dirección VLAN 23	192.168.23.1	Successful

Tabla 44. Conectividad de la red

La tabla 44 demuestra por medio del comando Ping los resultados de todos

Figura 65. Conectividad de la red



```
IOS Command Line Interface
Password:
Password:
S1>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.....
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/13/53 ms
S1>ping 192.168.21.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S1>ping 192.168.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1>
```

Fuente: Autor

En la figura 67 se verifica que la conectividad es correcta

Paso 3 . Configurar el protocolo de routing dinámico OSPF

Paso 5: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	router-id 2.2.2.2 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 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
Desactive la sumarización automática	no auto-summary

Tabla 45. OSPF en el R1

La tabla 45 muestra las tareas para configura en R1

Paso 6: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	router ospf 2 router-id 2.2.2.2 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0 network 10.10.10.10 0.0.0.255 area 0 passive-in passive-interface g0/1
Desactive la sumarización automática.	#No auto-summary

Tabla 46. Configurar OSPF en el R2

La tabla 46 especifica las configuraciones del OSPF en el R2

Paso 7: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	network 172.16.3.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback4 R3(config-router)#passive-interface loopback5 R3(config-router)#passive-interface loopback6 R3(config-router)#passive-interface loopback7
Desactive la sumarización automática.	#no auto-summary

Tabla 47. Tarea de configuración

La tabla 47 muestra la configuración de OSPFv3 en el R2

Figura 66. Configurar OSPF en el R2

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
L 192.168.6.1/32 is directly connected, Loopback6
R3#
R3#
R3#
R3#config t
Enter configuration commands, one per line. End with CNTRL/Z.
R3(config)#
R3(config-router)#version 2
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback4
% Invalid input detected at '^' marker.
R3(config-router)#passive-interface loopback4
R3(config-router)#passive-interface loopback5
R3(config-router)#passive-interface loopback6
R3(config-router)#no auto-summary
  
```

Fuente: Autor

La figura 68 muestra la Configuración de OSPF en el R2

Paso 8: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

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?	show ip ospf neig
¿Qué comando muestra solo las rutas OSPF?	show ip ospf interface
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip protocols

Tabla 48. Verificación OSPF

En la tabla 48 se evidencia las verificaciones de OSPF y las respectivas respuestas

Parte 3: 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:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar 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
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado</p> <pre>ip dhcp pool ENGR dns-server 10.10.10.10 default-router 192.168.23.1 network 192.168.23.0 255.255.255.0 ip domain-name ccna.com</pre>
--	---

Tabla 49. R1 como servidor de DHCP

En la tabla 49 muestra los elementos de configuración y las especificaciones

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 user webuser privilege 15 secret Cisco</p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>R2(config)#ip http server (comando no soportado por packet tracer)</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>#ip http authentication local</p>
<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: 209.165.200.229</p>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<pre>ip nat inside source static 10.10.10.10 209.165.200.229</pre>

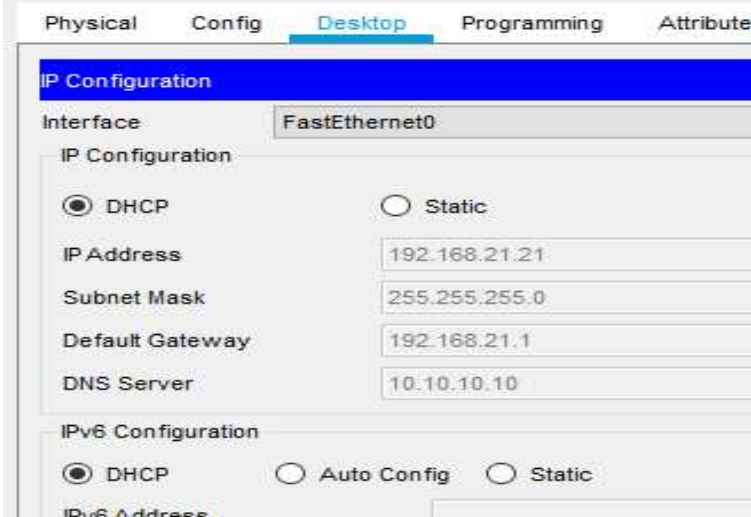
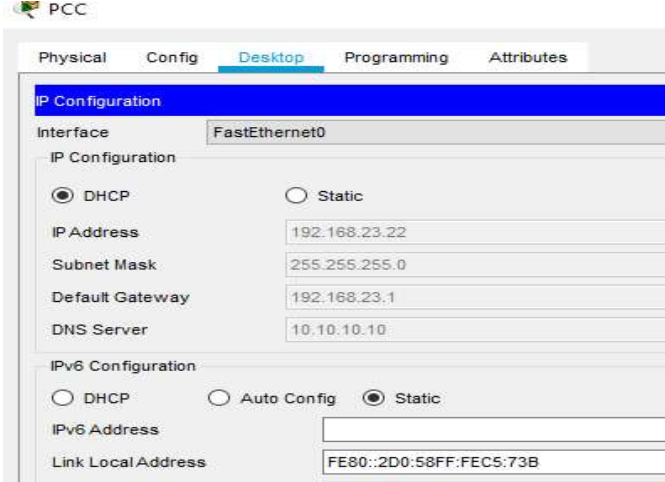
<p>Configurar la NAT dinámica dentro de una ACL privada</p>	<p>Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1: R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 (ver anexo 1): R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255</p>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228</p>
<p>Definir la traducción de NAT dinámica</p>	<p>ip nat pool Internet 209.165.200.229 209.165.200.228 netmask 255.255.255.248</p>

Tabla 50. NAT estática y dinámica

La tabla 50 muestra las tareas y especificaciones con respecto a la NAT estática y dinámica

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<p>Figura 67. Información de IP del servidor de DHCP</p>  <p>Fuente: Autor</p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<p>Figura 68. IP del servidor de DHCP</p> 

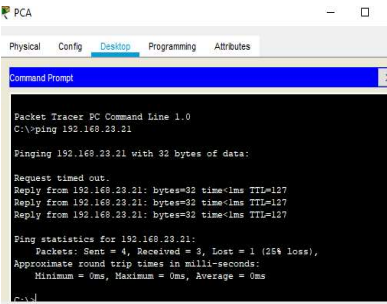
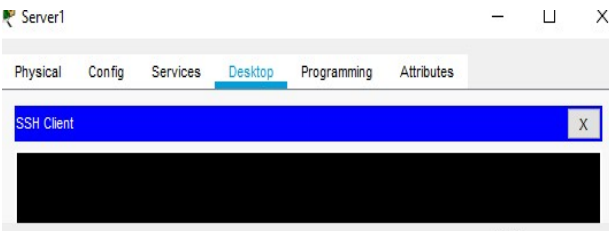
<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<p>Figura 69. PC-A pueda hacer ping a la PC-C</p>  <p>Fuente: Autor</p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	<p>Figura 70. Navegador web</p>  <p>Fuente: Autor</p>

Tabla 51. Protocolo DHCP y la NAT

En la tabla 51 se evidencian los protocolos DHCP y la NAT estática

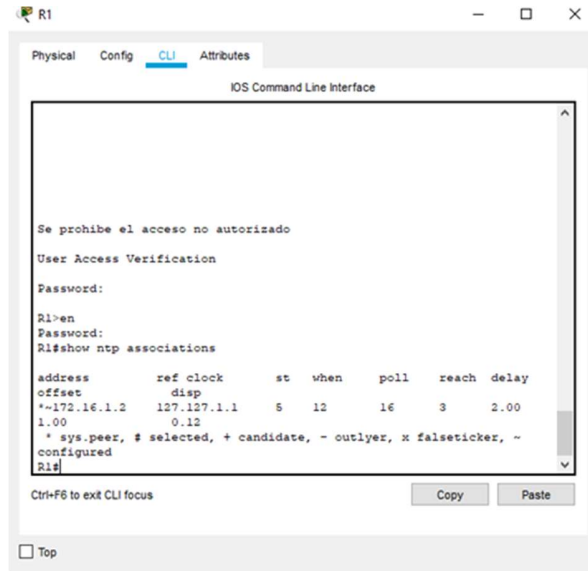
Parte 4: **Configurar NTP**

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: 5
Configurar R1 como un cliente NTP.	Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp server 209.165.200.229
Verifique la configuración de NTP en R1.	R1#show ntp associations

Tabla 52. Configurar NTP

En la tabla 52 se explican las configuraciones finales del NTP

Figura 71. NTP en R1



Fuente: Autor

La figura 73 evidencia en el IOS los commando aplicados.

Parte 5: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Tabla 53. Líneas VTY en el R2

La tabla 53 muestra las líneas VTY en R2 las cuales se deben configurar

Figura 72. NTP en R1



Fuente: Autor

La figura 74 muestra que No se permite: R2 From R3 por medio del telnet

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

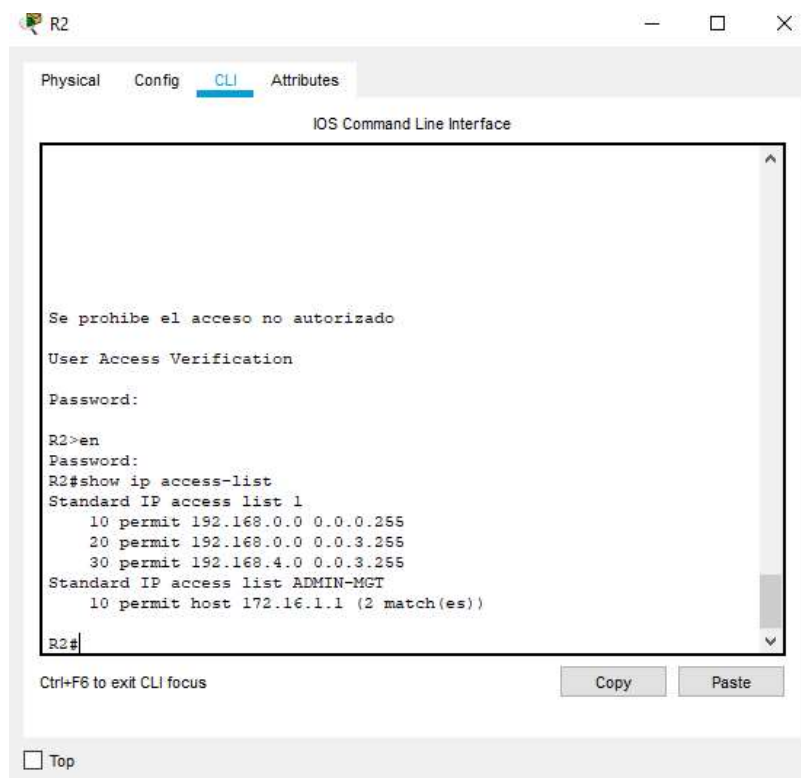
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router(config)#show access-list
Restablecer los contadores de una lista de acceso	R2#clear access-list counters 1
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	#Show run

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>#show ip nat translation</p> <p>Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>Show ip nat translations</p>

Tabla 54. Comando de CLI

En la tabla 54 se evidencian los comandos ingresados

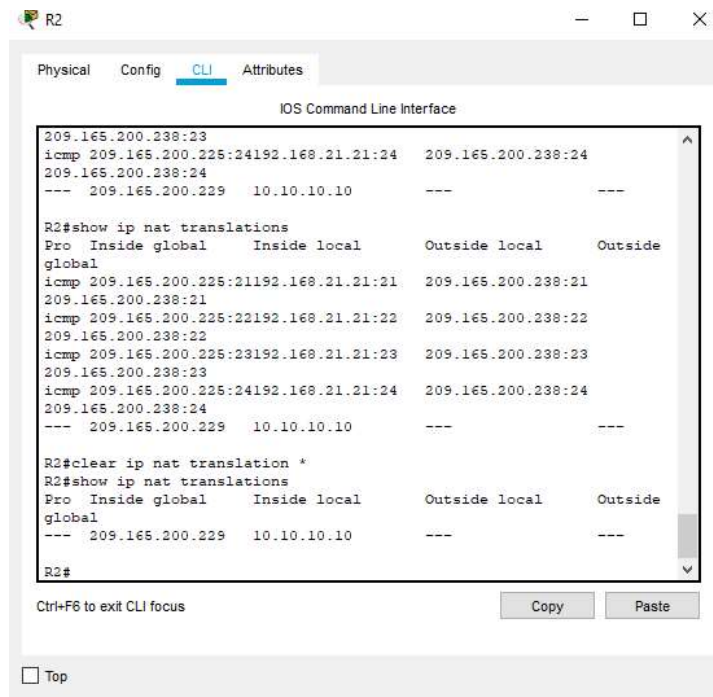
Figura 73. Comando de CLI



Fuente: Autor

En la figura 75 se evidencia el comando Cli con los respectivos comandos ingresados.

Figura 74. Comando de CLI



Fuente: Autor

En la figura 76 se evidencian los resultados finales con los Cli adecuados

CONCLUSIONES

Se pone en práctica los conocimientos adquiridos en el transcurso de el desarrollo de este seminario de profundización. La meta es profundizar en la conformación de redes de datos especialmente "Internet" y para ello se describen los dispositivos utilizados para una red y se explican con la simulación en el programa Packet Tracer como es el intercambio de paquetes y a la vez permite observar el comportamiento de la red creada. Este entorno es la base para el aprendizaje del í estudiante porque desarrolla las habilidades que necesita en esta sociedad tan acelerada en cuanto a toma de decisiones, pensamiento crítico, innovador siempre buscando dar solución a dificultades presentadas en todos los ámbitos de la vida diaria. Teniendo en cuenta las anteriores apreciaciones el Caso de estudio.

El uso de NAT puede ocultar el esquema de direccionamiento y la topología interna de la red, mejorando así el nivel de seguridad de la red. Además, también ayuda a reducir el consumo del espacio de direcciones IP públicas globales.

El protocolo de enrutamiento OSPF proporciona equilibrio de carga entre rutas de igual peso. Cuando el administrador especifica múltiples rutas al destino con el mismo costo, el protocolo OSPF distribuye el tráfico entre todas las rutas de la misma manera.

La asignación de DHCP de direcciones IP en la red puede optimizar los recursos porque asigna automáticamente direcciones de red reutilizables y otras configuraciones a diferentes hosts conectados.

BIBLIOGRAFÍA

Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. Recuperado 5 junio, 2019, de <https://byspel.com/configurar-servidor-dhcp-en-cisco-packet-tracer/>.

Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red.

JUANSA, J. Solucionando errores TCP/IP. 4 – Uno de los blogs de Juansa. (en línea). (5 octubre de 2018). Disponible en :<https://geeks.ms/juansa/2008/10/05/solucionando-errores-tcpip-4/>.

MARTINEZ, Victor. Configuración de RIPv2 (protocolo dinámico). (en línea). (25 febrero de 2013). Disponible en:<http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/>.

MARTINEZ, Victor. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. (en línea). (16 agosto de 2016). disponible en:<http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-router-cisco/>

Anexos

Escenario 1:

https://drive.google.com/file/d/1Ae6ye_POrijm2eM3uwUxl0jyYjo613ryn/view?usp=sharing

Escenario 2:

https://drive.google.com/file/d/1Ae6ye_POrijm2eM3uwUxl0jyYjo613ryn/view?usp=sharing

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Yeimy lorena cuviedes
 Universidad Nacional Abierta y A Distancia, ylcuviedesq@unadvirtual.edu.co

Resumen

A continuación se desarrolla un escenario planteado como pruebas de habilidades practicas esta exige los métodos aprendidos en el desarrollo para la solución de problemas, en el escenario uno debemos elaborar una relación entre los diferentes así como los comandos utilizados y la salida de estos, a su vez se debe realizar una codificación con los parámetros establecidos, a su vez se tiene que configurar los conmutadores mientras se verifica los como clientes, además de repetir los procedimientos en los puertos propuestos.

- *Palabras clave: Cisco systems, topología, interfaz.*

Abstract:

Next, a scenario proposed as practical skills tests is developed, this requires the methods learned in the development for solving problems, in scenario one we must develop a relationship between the different ones as well as the commands used and the output of these, at their own expense. Once a coding must be carried out with the established parameters, in turn, the switches must be configured while verifying them as clients, in addition to repeating the procedures on the proposed ports.

Keywords— Cisco systems, topology, interface.

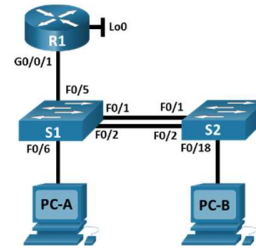


Tabla 55. Topología

Ilustración 1: Topología

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

Tabla de VLAN

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

Tabla 56. Tabla VLAN

Tabla de 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
	10.19.8.98 /29	10.19.8.97
S1 VLAN 4	2001.db8:acad:c::98 /64	No corresponde
	fe80::98	No corresponde
	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	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

Tabla 57. Asignación de direcciones

INTRODUCCIÓN

A continuación, usando los diferentes programas de simulación se describen paso a paso la configuración de los dispositivos de cada escenario, se exhibe su correcta operación ayudado de los comandos respectivos que permiten evidenciar su operatividad tanto en la utilización de protocolos, en el intercambio de información de sistemas autónomos, como la distribución de mediante el protocolo.

I. METODOLOGIA

Escenario 1. Topología

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla 58. Tabla tarea especificaciones

Se borra las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

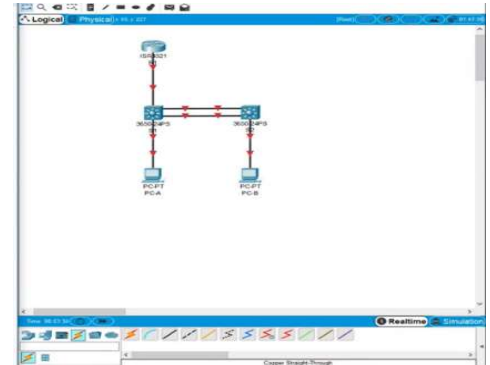


Figura 59. Topología del escenario

RESULTADOS

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

Tipo de cable	Punto de origen	Punto Destino
Cable directo	R1 g0/0/1	S1 g1/0/5
Cable directo	S1 g1/0/5	PC-A f0

Tabla 60. Punto de destino

```

PC-A
-----
Password:
R1>en
Password:
R1#conf term
Entere configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
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
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
R1(config)#
    
```

Figura 61. Muestra de resultados en PC-A

TABLA 3 DIRECCIONAMIENTO IP

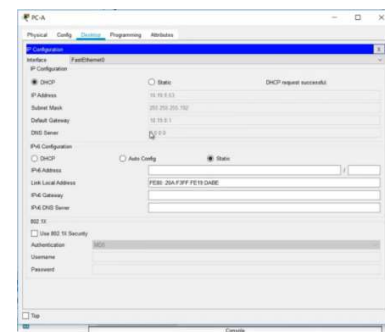


Figura 62. Direccionamiento IP

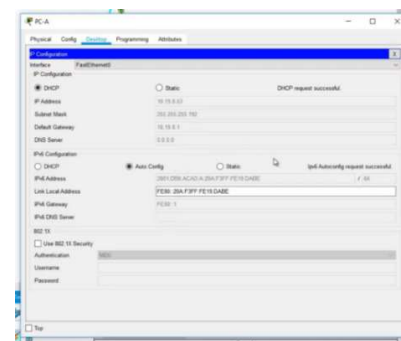


Figura 63. Direccionamiento Final

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**.

CONCLUSIONES

Se pone en práctica los conocimientos adquiridos en el transcurso del desarrollo de este seminario de profundización. La meta es profundizar en la conformación de redes de datos especialmente “Internet” y para ello se describen los dispositivos utilizados para una red y se explican con la simulación en el programa Packet Tracer como es el intercambio de paquetes y a la vez permite observar el comportamiento de la red creada. Este entorno es la base para el aprendizaje del estudiante porque desarrolla las habilidades que necesita en esta sociedad tan acelerada en cuanto a toma de decisiones, pensamiento crítico, innovador siempre buscando dar solución a dificultades presentadas en todos los ámbitos de la vida diaria. Teniendo en cuenta las anteriores apreciaciones el Caso de estudio

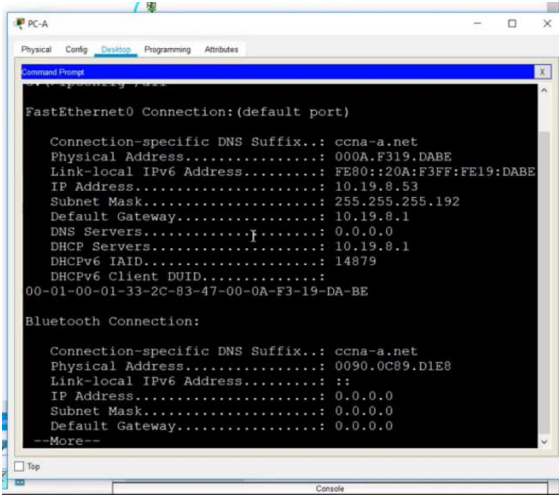


Figura 64. Pines de comprobación final

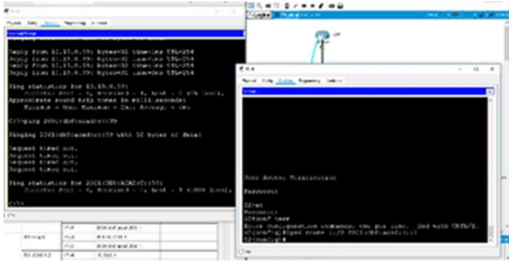


Tabla 65. Comprobación de la configuración

Por último, ya que se ha configurado la totalidad de dispositivos en la red; lo que se hace es la prueba de conexión entre los dispositivos según la tabla de verificación definida, la cual se hace mediante el comando ping desde la consola de comandos de cada computador en la red donde por medio del envío y recepción de paquetes se puede comprobar la conexión entre todos los dispositivos de la red y las restricciones de VLAN.

REFERENCIAS

Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. Recuperado 5 junio, 2019, de <https://byspel.com/configurar-servidor-dhcp-en-cisco-packet-tracer/>.

Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red.

JUANSA, J. Solucionando errores TCP/IP. 4 – Uno de los blogs de Juansa. (en línea). (5 octubre de 2018). Disponible en <https://geeks.ms/juansa/2008/10/05/solucionando-errores-tcpip-4/>.

MARTINEZ, Victor. Configuración de RIPv2 (protocolo dinámico). (en línea). (25 febrero de 2013). Disponible en: <http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/>.

MARTINEZ, Victor. (2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. (en línea). (16 agosto de 2016). disponible en: <http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-router-cisco/>

BIOGRAFÍA



Yeimy Cuvides (1992) nació en Ocaña (Colombia) el 24 de octubre de 1992. Empezó a estudiar en la Universidad Nacional Abierta y a Distancia UNAD en el año 2015 y actualmente se encuentra haciendo su diplomado en Profundización Cisco.

Actualmente cuenta con experiencia como analista financiera.