SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

NAYIBE ALEXANDRA IJAJI ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2022

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

NAYIBE ALEXANDRA IJAJI ORTIZ

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

DIRECTOR:
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2022

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

SAN JUAN DE PASTO, 26 de octubre de 2022

AGRADECIMIENTOS

Agradezco a Dios, por permitir lograr mis objetivos y superar todos los obstáculos presentados en mi carrera universitaria.

A mis padres y hermana, por su esfuerzo, paciencia y apoyo incondicional que permitieron lograr esta meta.

A mis tutores de la UNAD, por brindarme su apoyo y conocimientos en este proceso de formación profesional.

Por último, a mi peludito fiel que, durante todas las noches de desvelo y momentos de soledad, su compañía fue motivación para no sentirme sola y estudiar a gusto, gracias, Joyce.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RIPV2: Es un protocolo de puerta de enlace interno, usado en los routers con los que se intercambia información de redes en dispositivos conectados.[1]

SWITCHING: Está enfocado a dispositivos Switch, toma la información y reenvía a través de sus puertos de comunicación utilizando una serie de protocolos como VLAN, VTP, RSTP y PVSTP para optimizar y mejorar el flujo de datos de las redes LAN. [2]

ROUTING: Está enfocado a los dispositivos Router, encamina paquetes a través de las redes y para realizar él envió de esta información los Router utilizan OSPF, RIP y EIGRP que son protocolos de enrutamiento dinámico. [3]

VTP: Protocolo utilizado para la distribución y sincronización de la información de bases de datos VLAN, configurado a través de una red conmutada; además minimiza las configuraciones y configuraciones erróneas e inconsistencias que pueden generar varios problemas, como nombres de VLAN duplicados e incorrectos. [4]

NAT: Es una traducción de direcciones de red, que permite la comunicación de una red privada con una red pública para generar ahorro de direcciones IP, encontramos varios tipos de Nat estático, dinámico, sobrecarga y solapamiento. [5]

ETHERCHANNEL: Es una tecnología de agregación de enlaces que agrupa varios enlaces físicos Ethernet en un único enlace lógico. Se utiliza para proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre conmutadores, enrutadores y servidores. [6]

[1] Wikipedia, Wikipedia®, Routing Informtaion Protocol. (2022)
[2] Cisco, Networking Academy, Switching, Routing, y Wireless Essentials. (2022)
[3] Cisco, Networking Academy, Switching, Routing, y Wireless Essentials. (2022)
[4] Cisco, Networking Academy, Switching, Routing, y Wireless Essentials. (2022)
[5] Cisco, Networking Academy, Direccionamiento IP (2022)
[6] Cisco, Networking Academy, Switching, Routing, y Wireless Essentials. (2022)

RESUMEN

La prueba de habilidades permitirá el desarrollo de 2 escenarios, donde identificará conocimientos y competencias adquiridas durante el curso de profundización de CISCO CCNA

El primer escenario abordará al diseño de pequeñas redes LAN, trabajado solo con direccionamiento IPV4; incluyendo configuraciones básicas como claves encriptadas, banner, interfaces mediante el subneteo etc. Cada LAN tendrá asociado a un dispositivo electrónico (host) para hacer pruebas de conectividad.

Para el segundo escenario se evidenciará los protocolos de Conmutación y enrutamiento, donde se implementará la comunicación de diferentes VLAN en switches de capa 3, asignando puertos troncales en cada uno de estos.

Además, el proceso tanto para el escenario 1 como para el escenario 2 se llevará a cabo mediante el simulador Packet Tracer

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

ABSTRACT

The skills test will allow the development of 2 scenarios, where it will identify knowledge and skills acquired during the CISCO CCNA deepening course

The first scenario will address the design of small LAN networks, working only with IPV4 addressing; including basic configurations such as encrypted keys, banners, interfaces through subnetting, etc. Each LAN will have an electronic device (host) associated with it to carry out connectivity tests.

For the second scenario, the switching and routing protocols will be evidenced, where the communication of different VLANs will be implemented in layer 3 switches, assigning trunk ports in each of these.

In addition, the process for both scenario 1 and scenario 2 will be carried out using the Packet Tracer simulator.

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

INTRODUCCIÓN

En el siguiente trabajo se encuentra el desarrollo del escenario 1 y 2, donde se trabaja con tecnología Cisco, a través del programa Packet Tracer, un simulador para diseñar y construir diferentes topologías de red, configurar dispositivos de red y evaluar su comportamiento.

Para el escenario 1, se enfoca en el diseño de redes LAN pequeñas, y se inicia con la configuración el direccionamiento IPV4, donde se observan los siguientes dispositivos Router, Switch y host; se configura términos básicos como inicio de sesión, contraseñas cifradas, mascara de subred e IP, nombre de equipo, contraseñas de acceso etc.

En el escenario 2, se trabaja con los dos direccionamientos IPV4 e IPV6, donde son implementados en un Router, 2 Switch de capa 3 y 2 host, en estos se configuran parámetros de Etherchannel y port-security

Ambos escenarios verifican la conectividad de extremo a extremo y el funcionamiento de la red en conjunto en los dispositivos host (pc) con el comando ping.

1. ESCENARIO 1

Escenario: En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un Router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El Router y el switch también deben administrarse de forma segura.

Topología

Figura 1. Escenario 1

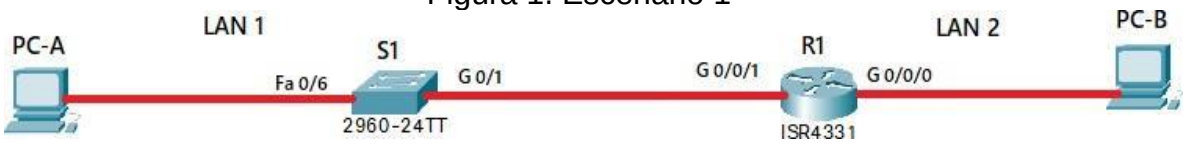
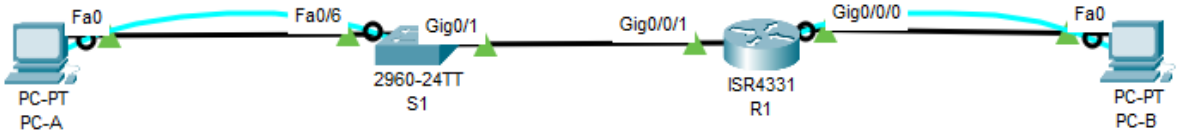


Figura 2. Simulación de escenario 1



1.1. Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1. Tabla de direccionamiento escenario 1

Ítem	**Requerimiento**
Dirección de Red	**Fórmula:** 2^N (número de bits)-2(Dirección y Broadcast) ≥ No Host LAN 1 2^6 -2 ≥ **62** = 172.1.3.64/26 172.1.3.65/26 - 172.1.3.126/26 LAN 2 2^5 -2 ≥ **30** = 172.1.3.0/27 172.1.3.1/27-172.1.3.30/27
Requerimiento de host Subred LAN1	**60 =** 62 host 172.1.3.64/26 255.255.255.192

Requerimiento de host Subred LAN2	**20 =** 30 host 172.1.3.0/27 255.255.255.224
R1 G0/0/1	Última dirección de host de la subred LAN1 - 172.1.3.126/26
R1 G0/0/0	Última dirección de host de la subred LAN2 -172.1.3.30/27
S1 SVI	Segunda dirección de host de la subred LAN1 - 172.1.3.66/26
PC-A	Décima dirección de host de la subred LAN1 - 172.1.3.74/26
PC-B	Décima dirección de host de la subred LAN2 - 172.1.3.10/27

1.2. Configurar los aspectos básicos:

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

1.2.1. Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración Router 1 escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain-name ccna-sa.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass R1(config)#
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)#username admin privilege 15 secret admin1pass

Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configurar un banner MOTD	R1(config)#banner motd #R1 - Nayibe Alexandra Ijaji Ortiz - Ingeniera de sistemas#
Configuración de interface G0/0/0 172.1.3.30/27 255.255.255.224	R1(config)#interface gigabitEthernet0/0/0 R1(config-if)#ip address 172.1.3.30 255.255.255.224 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up R1(config-if)#
Configuración de interface G0/0/1 172.1.3.126/26 255.255.255.192	R1(config)#interface gigabitEthernet0/0/1 R1(config-if)#ip address 172.1.3.126 255.255.255.192 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up R1(config-if)#
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa *Mar 1 1:19:16.304: RSA key size needs to be at least 768 bits for ssh version 2 *Mar 1 1:19:16.304: %SSH-5-ENABLED: SSH 1.5 has been enabled % You already have RSA keys defined named R1.ccna-sa.com .

	% Do you really want to replace them? [yes/no]: yes The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: **1024** % Generating **1024** bit RSA keys, keys will be non-exportable...[OK]

1.2.2. Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Configuración Switch 1 escenario 1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#
Apagar todos los puertos sin usar	S1(config)#interface range fa0/1-4,F0/7-24, G0/1-2 S1(config-if-range)#shutdown
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un banner MOTD	S1(config)#banner motd #S1 - Nayibe Alexandra Ijaji Ortiz - Ingeniera de sistemas# S1(config)#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: **1024** % Generating **1024** bit RSA keys, keys will be non-exportable...[OK]
Configure la interfaz de administración (SVI) en VLAN1	S1(config)#interface vlan 1 S1(config-if)#ip address 172.1.3.66 255.255.255.192 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#exit S1(config)#ip default-gateway 172.1.3.126 S1(config)#

1.3. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 4. Configuración PC-A escenario 1

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0060.479D.2462
Dirección IPv4	172.1.3.74
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.1.3.126

Figura 3. Configuración PC-A escenario 1

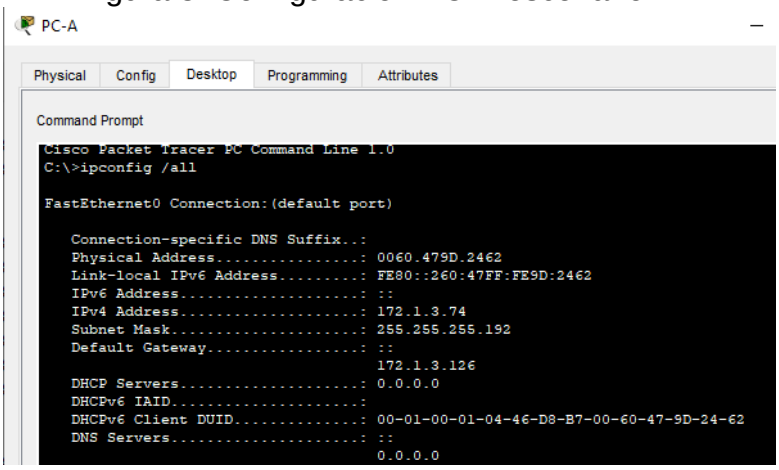
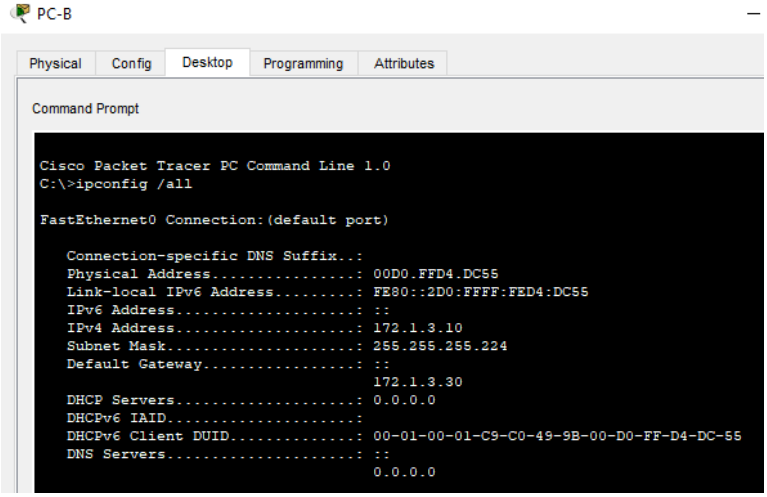


Tabla 5. Configuración PC-B escenario 1

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	00D0.FFD4.DC55
Dirección IPv4	172.1.3.10
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.1.3.30

Figura 4. Configuración PC-B escenario 1



1.4. Probar y verificar la conectividad de extremo a extremo

Utilice el comando ping para probar la conectividad entre todos 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:

Tabla 6. Verificación de Conectividad escenario 1

Desde	PC-A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.1.3.30	C:\>ping 172.1.3.30 Pinging 172.1.3.30 with 32 bytes of data: Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Ping statistics for 172.1.3.30: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
	R1 G0/0/1	172.1.3.126	C:\>ping 172.1.3.126 Pinging 172.1.3.126 with 32 bytes of data: Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Reply from 172.1.3.126: bytes=32 time=2ms TTL=255 Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Ping statistics for 172.1.3.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms
	S1 VLAN 1	172.1.3.66	C:\>ping 172.1.3.66 Pinging 172.1.3.66 with 32 bytes of data:

			Request timed out. Reply from 172.1.3.66: bytes=32 time<1ms TTL=255 Reply from 172.1.3.66: bytes=32 time<1ms TTL=255 Reply from 172.1.3.66: bytes=32 time<1ms TTL=255 Ping statistics for 172.1.3.66: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
	PC-B	172.1.3.10	C:\>ping 172.1.3.10 Pinging 172.1.3.10 with 32 bytes of data: Request timed out. Reply from 172.1.3.10: bytes=32 time<1ms TTL=127 Reply from 172.1.3.10: bytes=32 time<1ms TTL=127 Reply from 172.1.3.10: bytes=32 time<1ms TTL=127 Ping statistics for 172.1.3.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>
PC-B	R1 G0/0/0	172.1.3.30	C:\>ping 172.1.3.30 Pinging 172.1.3.30 with 32 bytes of data: Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255 Reply from 172.1.3.30: bytes=32 time<1ms TTL=255

			Ping statistics for 172.1.3.30: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
	R1 G0/0/1	172.1.3.126	C:\>ping 172.1.3.126 Pinging 172.1.3.126 with 32 bytes of data: Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Reply from 172.1.3.126: bytes=32 time<1ms TTL=255 Ping statistics for 172.1.3.126: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
	S1 VLAN1	172.1.3.66	C:\>ping 172.1.3.66 Pinging 172.1.3.66 with 32 bytes of data: Request timed out. Request timed out. Reply from 172.1.3.66: bytes=32 time<1ms TTL=254 Reply from 172.1.3.66: bytes=32 time<1ms TTL=254 Ping statistics for 172.1.3.66: Packets: Sent = 4, Received = 2, Lost = 2 (50% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Figura 5. Ping desde PC-A a R1 escenario 1

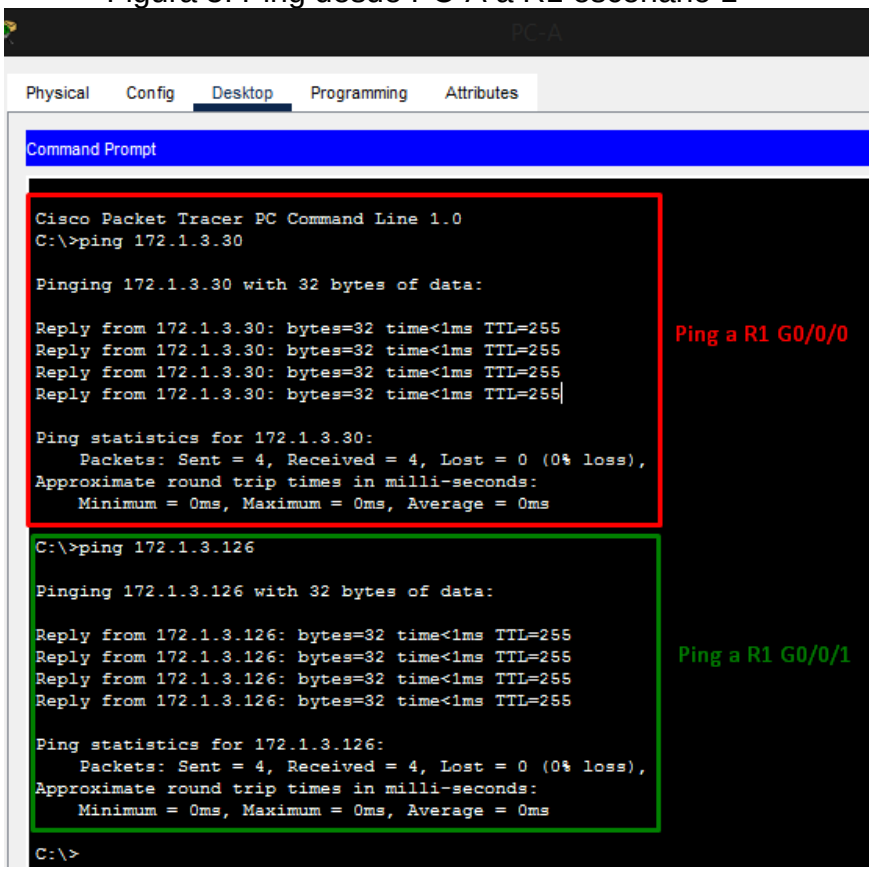


Figura 6. Ping desde PC-A a S1

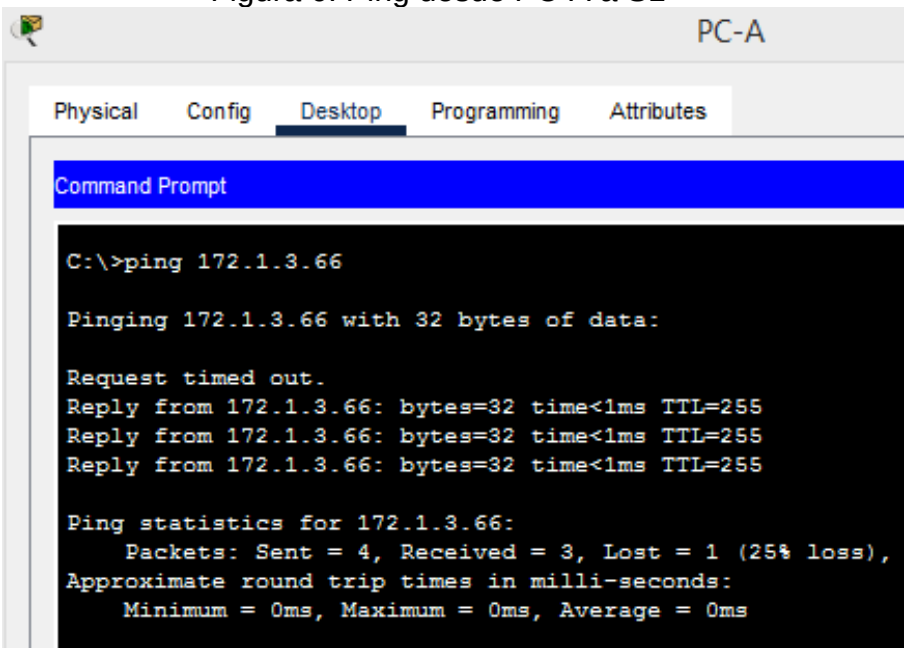


Figura 7. Ping desde PC-A a PC-B escenario 1

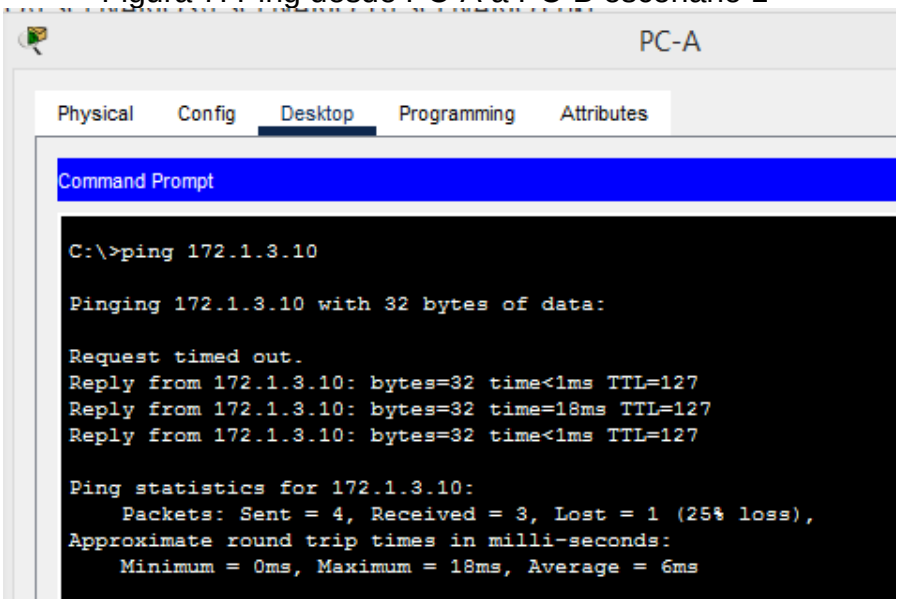


Figura 8. Ping desde PC-B a R1 escenario 1

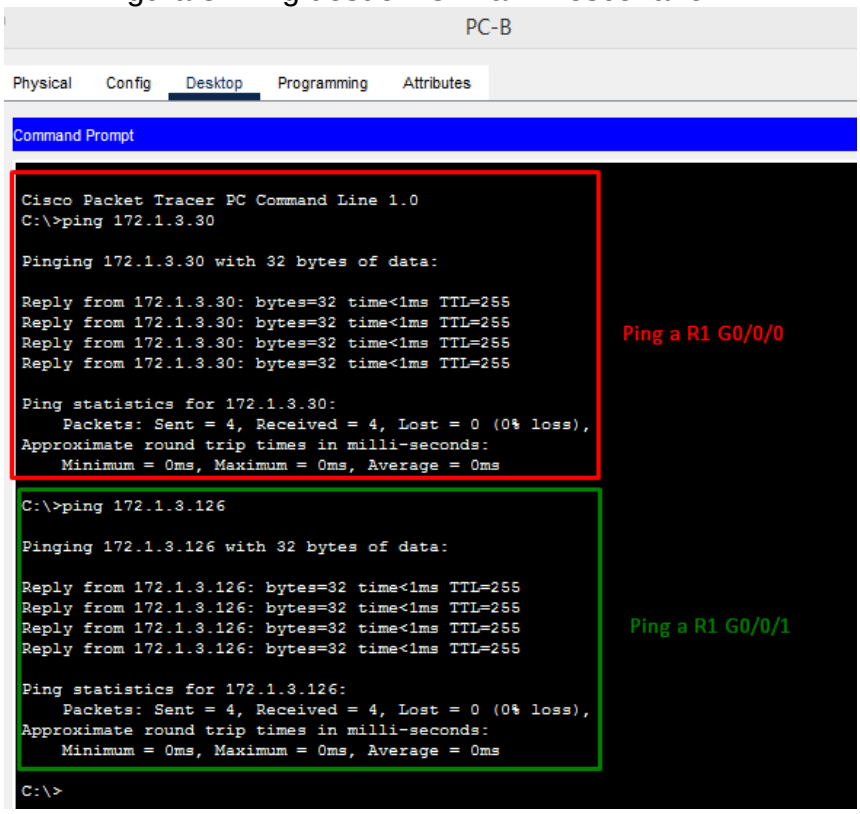
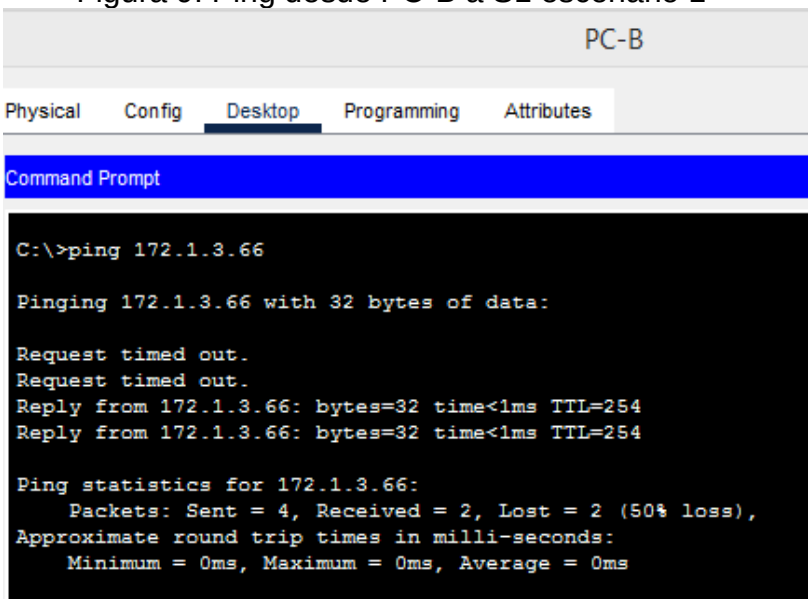


Figura 9. Ping desde PC-B a S1 escenario 1



2. ESCENARIO 2

Topología

Figura 10. Escenario 2

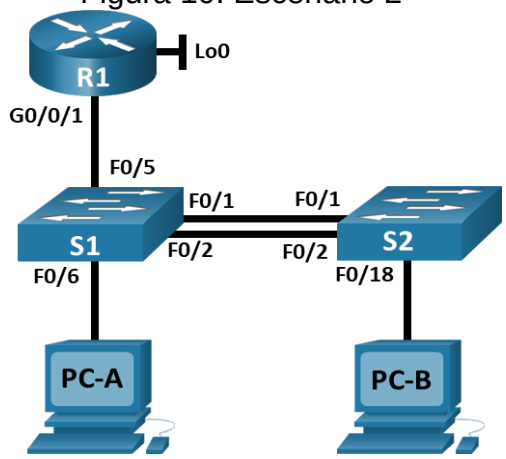
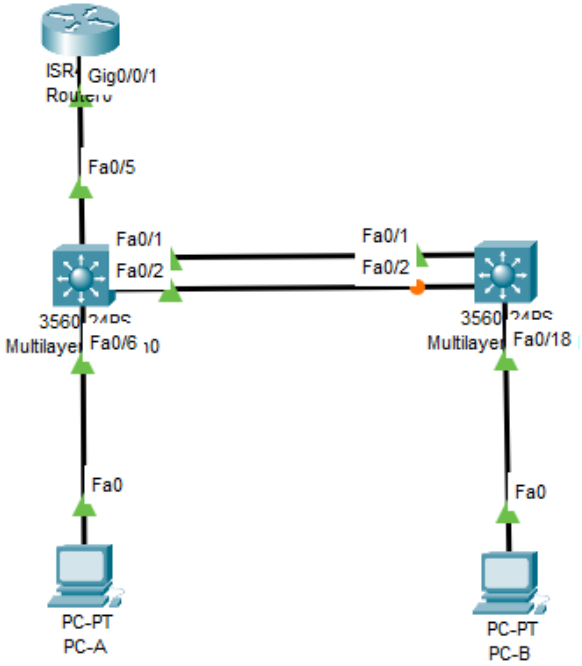


Figura 11. Simulación escenario 2



En este 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. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

Tabla 7. Nombres VLAN escenario 2

VLAN	Nombre de la VLAN
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Tabla de asignación de direcciones

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberá reemplazarlos por los últimos dos dígitos de su número de identificación.

Tabla 8. Asignación de direcciones escenario 2

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.1.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.1.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.1.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1/64	No corresponde
S1 VLAN 40	10.1.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98/64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.1.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b::50 /64	fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos 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.

R1

Router>enable

Router#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#reload

Proceed with reload? [confirm]

Initializing Hardware ...

S1

Switch>enable

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#reload

Proceed with reload? [confirm]

S2

Switch>enable

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#reload
Proceed with reload? [confirm]

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

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuración R1 escenario 2

Tarea	Especificación
Desactivar la búsqueda DNS	Router#configure t Enter configuration commands, one per line. End with CNTL/Z. Router(config)# % Unknown command or computer name, or unable to find computer address Router(config)#no ip domain-lookup
Nombre del router R1	Router(config)#hostname R1 R1(config)#
Nombre de dominio ccna-sa.com	R1(config)#ip domain-name ccna-sa.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado class	R1(config)#enable secret class R1(config)#
Contraseña de acceso a la consola cisco	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login
Establecer la longitud mínima para las contraseñas 5 caracteres	R1(config)#security passwords min-length 5 R1(config)#
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	R1(config)#username admin privilege 15 secret admin1pass R1(config)#

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	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 R1(config)#
Configure un MOTD Banner Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	R1(config)#banner motd #R1 Nayibe Alexandra Ijaji Ortiz Ingenieria de Sistemas# R1(config)#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.	R1#configure t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#interface gi0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description Docente R1(config-subif)#ip address 10.1.8.1 255.255.255.192 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-subif)#exit R1(config)# R1(config)#interface gi0/0/1.30 R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#ip address 10.1.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Estudiantes R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gi0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description Invitados R1(config-subif)#ip address 10.1.8.97 255.255.255.248

	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 R1(config-subif)#exit R1(config)#interface gi0/0/1.56 R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#description Native R1(config-subif)#exit R1(config)#interface gi0/0/1 R1(config-if)#no shutdown
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	R1(config)#interface lo0 R1(config-if)#description Loopback0 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
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#crypto key generate RSA The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 10. Configuración S1 escenario 2

Tarea	Especificación
Habilitar la plantilla de ipv6 con sdm prefer	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use 'show sdm prefer' to see what SDM preference is currently active. Switch(config)#exit

	Switch#reload Switch#reload System configuration has been modified. Save? [yes/no]:no Proceed with reload? [confirm]
Desactivar la búsqueda DNS.	Switch>enable Switch#configure t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1
Nombre de dominio ccna-sa.com	S1(config)#ip domain-name ccna-sa.com S1(config)#
Contraseña cifrada para el modo EXEC privilegiado class	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola cisco	S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin privilege 15 secret admin1pass S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Configurar un MOTD Banner Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	S1(config)#banner motd #S1 Nayibe Alexandra Ijaji Ortiz Ingenieria de Sistemas# S1(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#crypto key generate RSA The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80::98 para Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 40 S1(config-if)#ip address 10.1.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.1.8.97 para IPv4	S1(config)#ip default-gateway 10.1.8.97 S1(config)#

Tabla 11. Configuración S2 escenario 2

Tarea	Especificación
Habilitar la plantilla de ipv6 con sdm prefer	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default Changes to the running SDM preferences have been stored, but cannot take effect until the next reload. Use 'show sdm prefer' to see what SDM preference is currently active. Switch(config)#exit Switch#reload Switch#reload System configuration has been modified. Save? [yes/no]:no Proceed with reload? [confirm]
Desactivar la búsqueda DNS.	Switch>enable Switch#configure t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch S2	Switch(config)#hostname S2
Nombre de dominio ccna-sa.com	S2(config)#ip domain-name ccna-sa.com S2(config)#

Contraseña cifrada para el modo EXEC privilegiado class	S2(config)#enable secret class S2(config)#
Contraseña de acceso a la consola cisco	S2(config)#line con 0 S2(config-line)#password cisco S2(config-line)#login
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S2(config)#username admin privilege 15 secret admin1pass S2(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vt 0 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 15 S2 (config-line)#transport input ssh S2 (config-line)#login local
Cifrar las contraseñas de texto no cifrado	S2 (config)#service password-encryption
Configurar un MOTD Banner Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	S2(config)#banner motd #S2 Nayibe Alexandra Ijaji Ortiz Ingenieria de Sistemas# S2(config)#
Generar una clave de cifrado RSA Módulo de 1024 bits	S2(config)#crypto key generate RSA The name for the keys will be: S2.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80::99 para Establecer la dirección IPv6 de capa 3	S2(config)#interface vlan 40 S2(config-if)#ip address 10.1.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit

Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.1.8.97 para IPv4	S2 (config)#ip default-gateway 10.1.8.97 S2(config)#

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Creación VLAN S1 escenario 2

Tarea	Especificación
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#vlan 56 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#interface range fa0/1-2, fa0/5 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk Native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1
Configurar el puerto de acceso de host para VLAN 20 Interface F0/6	S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso Permitir 4 direcciones MAC	S1(config)#interface fa0/6 S1(config-if)#switchport port-security maximum 4 S1(config-if)#

Proteja todas las interfaces no utilizadas Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description Sin_uso S1(config-if-range)#shutdown

Paso 5: Configure el S2.

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

Tabla 13. Creación VLAN S2 escenario 2

Tarea	Especificación
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S2(config)#vlan 20 S2(config-vlan)#Name Docentes S2(config-vlan)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#vlan 40 S2(config-vlan)#Name Invitados S2(config-vlan)#vlan 50 S2(config-vlan)#Name Usuarios S2(config-vlan)#vlan 56 S2(config-vlan)#Name Native
Crear troncos 802.1Q que utilicen la VLAN 56 nativa Interfaces F0/1 y F0/2	S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S2(config)#interface range fa0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 S2(config-if-range)#interface port-channel 1
Configurar el puerto de acceso del host para la VLAN 30 Interfaz F0/18	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30
Configure port-security en los access ports permite 4 MAC addresses	S2(config)#interface fa0/18 S2(config-if)#switchport port-security maximum 4
Asegure todas las interfaces no utilizadas.	S2(config-if)#interface range fa0/3-17, fa0/19-24, gi0/1-2

Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description Sin_uso S2(config-if-range)#shutdown

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Habilitar PE a VLAN 20 y 30 R1 escenario 2

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	Password: R1#conf t Enter 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)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 20 Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp excluded-address 10.1.8.1 10.1.8.52 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config)#network 10.1.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.1.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#exit R1(config)#
Configurar DHCP IPv4 para VLAN 30 Cree un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del	R1(config)#ip dhcp excluded-address 10.1.8.65 10.1.8.84 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config)#network 10.1.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.1.8.65 R1(dhcp-config)#domain-name unad-ccna-sb.net R1(dhcp-config)#exit R1(config)#

router para la subred involucrada	

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**.

Tabla 15. Configuración PC-A escenario 2

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000A.F328.7735
Dirección IPV4	10.1.8.53
Dirección IPV6	2001:DB8:ACAD:A::50
Máscara de subred IPV4	255.255.255.192
Máscara de subred IPV6	64
Gateway predeterminado IPV4	10.1.8.1
Gateway predeterminado IPv6	FE80::1

Figura 12. Configuración PC-A escenario 2

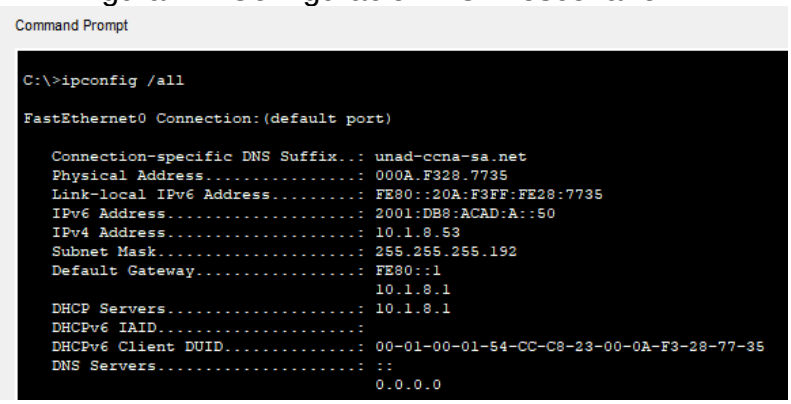
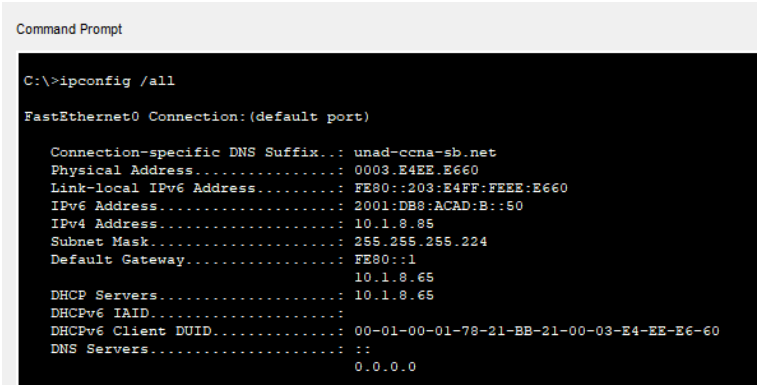


Tabla 16. Configuración PC-B escenario 2

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	0003.E4EE.E660
Dirección IPV4	10.1.8.85
Dirección IPV6	2001:DB8:ACAD:B::50
Máscara de subred IPV4	255.255.255.224

Máscara de subred IPV6	64
Gateway predeterminado	10.1.8.65
Gateway predeterminado IPv6	FE80::1

Figura 13. Configuración PC-B escenario 2

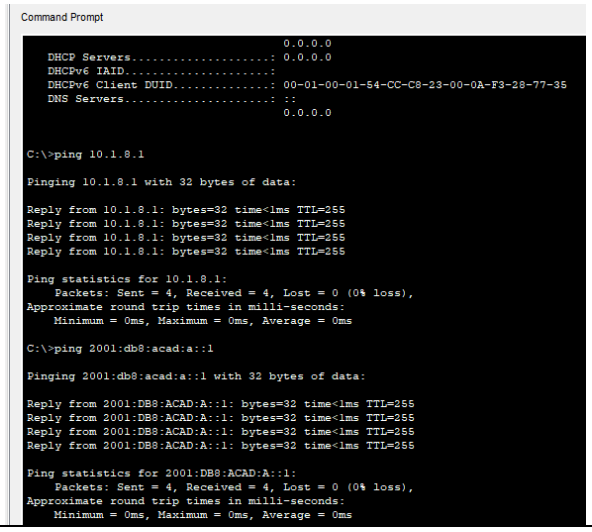


Parte 3: Probar y verificar la conectividad de extremo a extremo

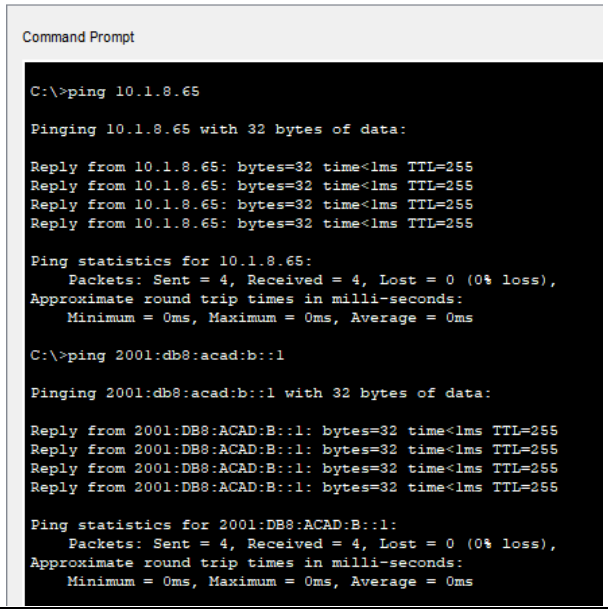
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

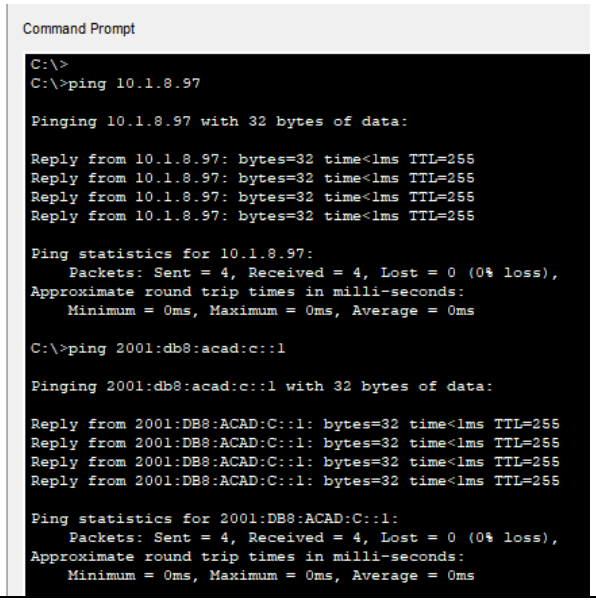
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Pruebas de conectividad de extremo a extremo escenario 2

Desde	**A**		**Dir IP**	**Resultados de ping**
PC-A	R1, G0/0/1.20	IPv4	10.1.8.1	Figura 14. Ping a R1 1.20 IPV4 e IPV6 desde PC-A escenario 2 
		IPv6	2001:db8:acad:a::1	

	R1, G0/0/1.30	IPv4	10.1.8.65	Figura 15. Ping a R1 1.30 IPV4 e IPV6 desde PC-A escenario 2
		IPv6	2001:db8:acad:b::1	
	R1, G0/0/1.40	IPv4	10.1.8.97	Figura 16. Ping a R1 1.40 IPV4 e IPV6 desde PC-A
		IPv6	2001:db8:acad:c::1	





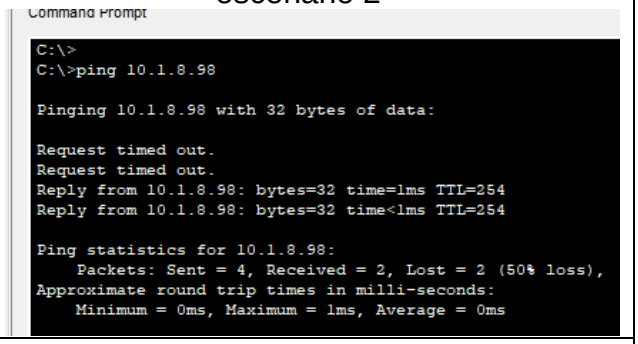
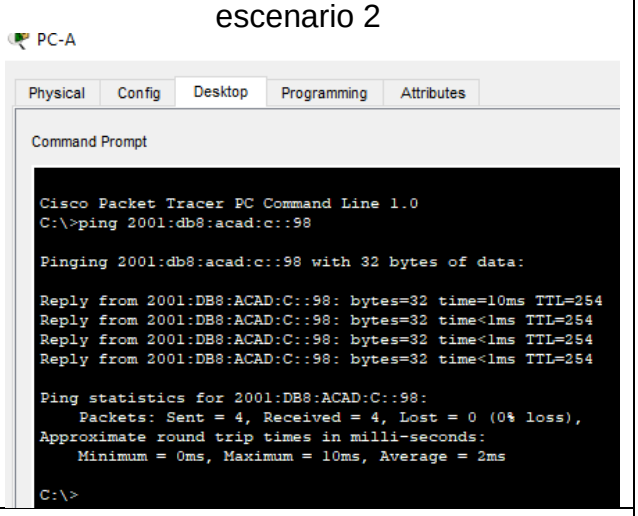
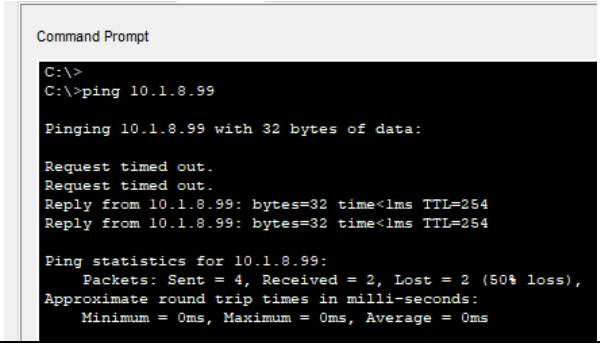
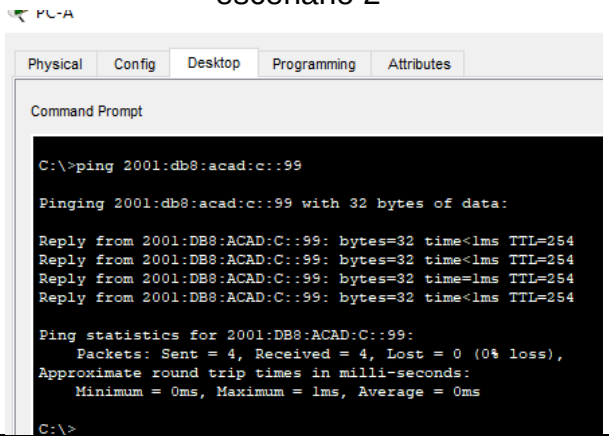
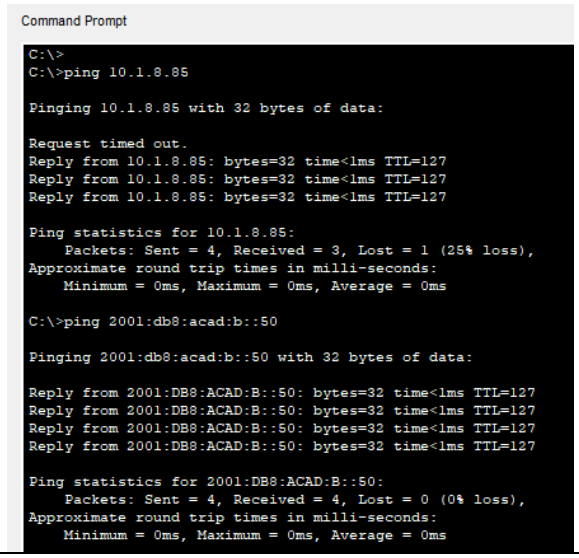
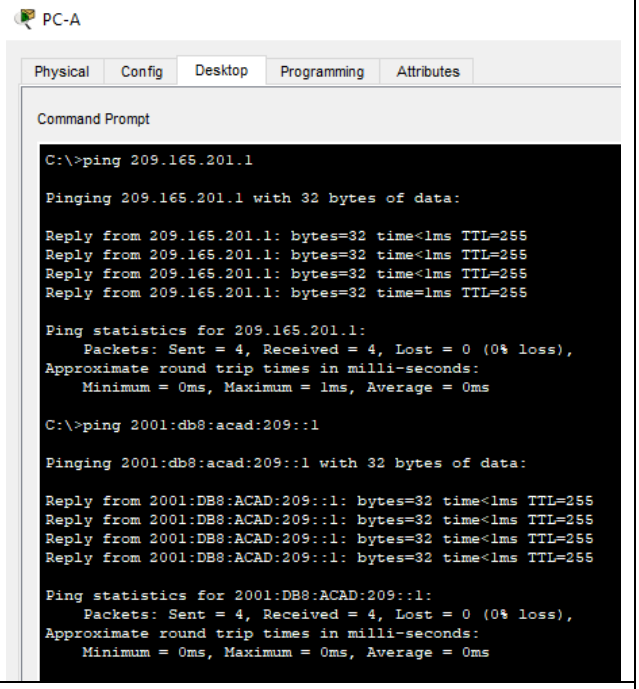
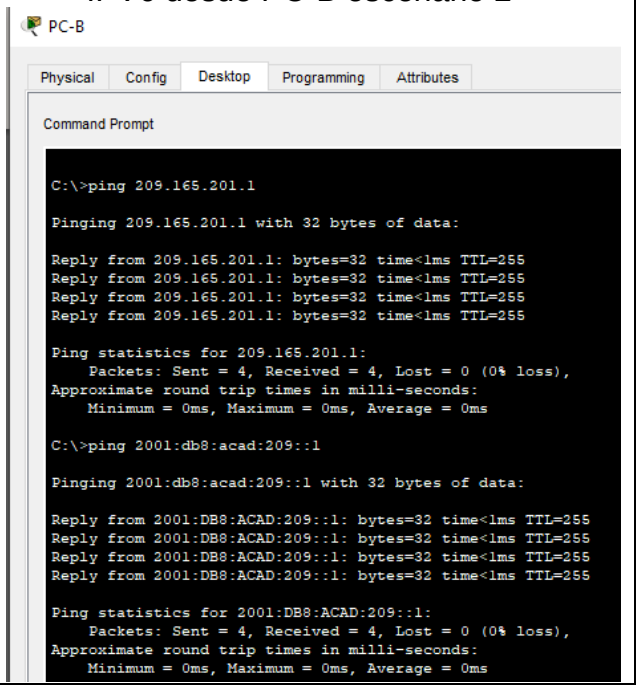
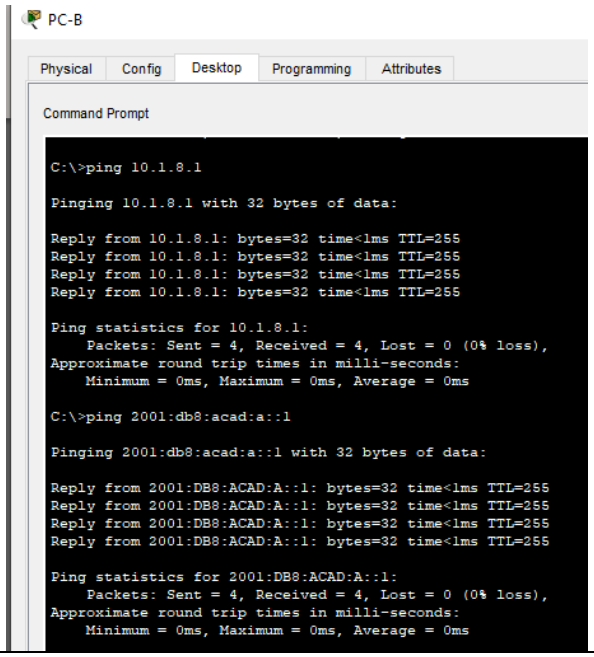
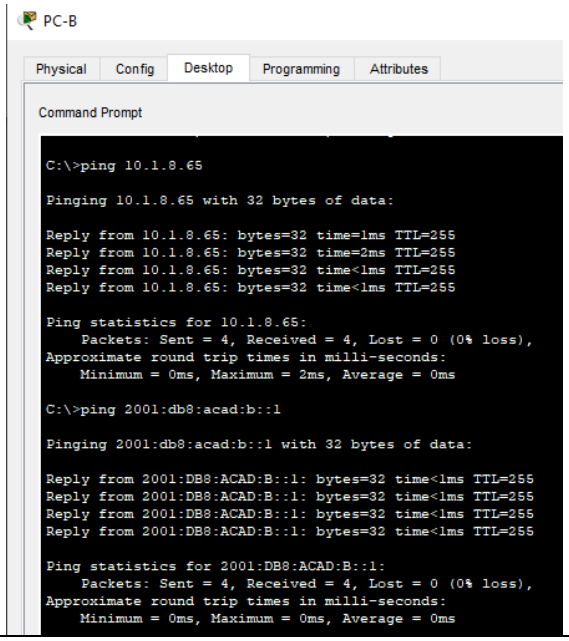
<table>
<tr><td rowspan="3"></td><td rowspan="2">S1, VLAN 40</td><td>IPv4</td><td>10.1.8.98</td><td>Figura 17. Ping a S1 IPV4 desde PC-A escenario 2
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::98</td><td>Si registramos el siguiente comando IPv6 route ::/0 2001:db8:acad:c::1 para habilitar la PE de IPV6 habrá respuesta, más sin embargo perderá conectividad PE de IPV4

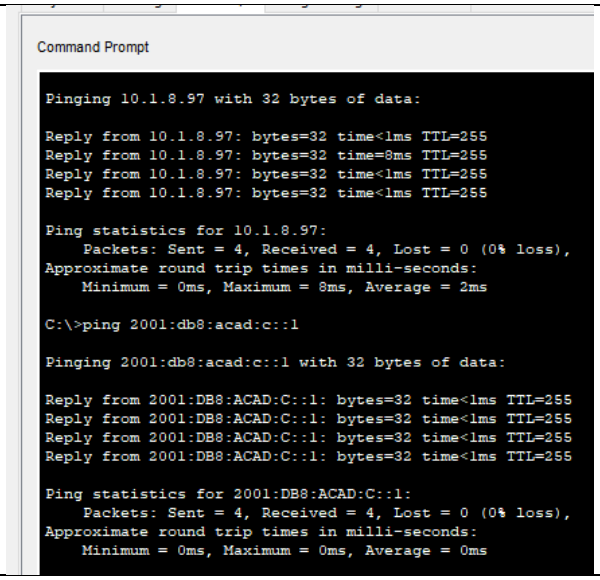
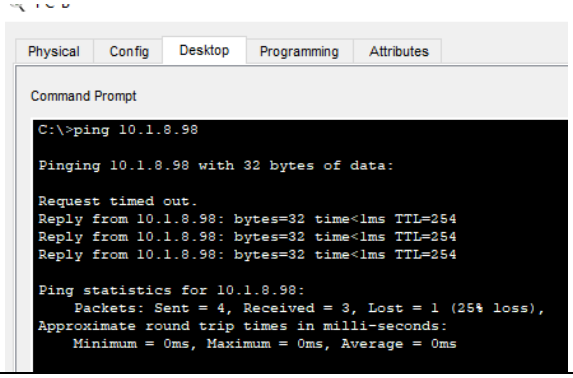
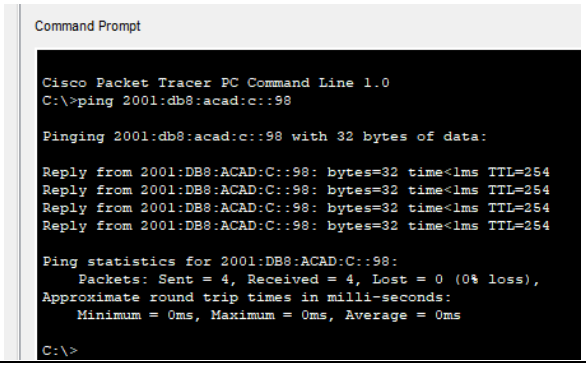
Figura 18. Ping a S1 IPV6 desde PC-A escenario 2
 
</td></tr>
<tr><td>S2, VLAN 40</td><td>IPv4</td><td>10.1.8.99</td><td>Figura 19. Ping a S2 IPV4 desde PC-A escenario 2
 
</td></tr>
</table>

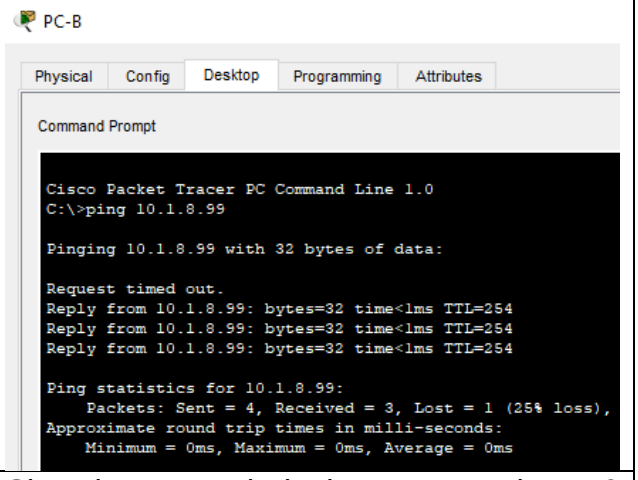
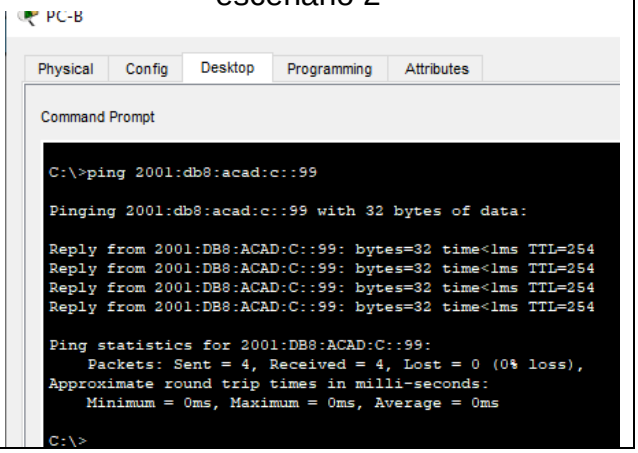
<table>
<tr><td rowspan="3"></td><td></td><td>IPv6</td><td>2001:db8:acad:c::99</td><td>Si registramos el siguiente comando IPv6 route ::/0 2001:db8:acad:c::1 para habilitar la PE de IPV6 habrá respuesta, más sin embargo perderá conectividad PE de IPV4

Figura 20. Ping a S2 IPV6 desde PC-A escenario 2
 
</td></tr>
<tr><td rowspan="2">PC-B</td><td>IPv4</td><td>10.1.8.85</td><td rowspan="2">Figura 21. Ping a PC-B IPV4 e IPV6 desde PC-A escenario 2
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b::50</td></tr>
</table>

	R1 Bucle 0	IPv4	209.165.201.1	Figura 22. Ping a R1 Bucle 0 IPV4 e IPV6 desde PC-A escenario 2 
		IPv6	2001:db8:acad:209::1	
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Figura 23. Ping a R1 Bucle 0 IPV4 e IPV6 desde PC-B escenario 2 
		IPv6	2001:db8:acad:209::1	

	R1, G0/0/1.20	IPv4	10.1.8.1	Figura 24. Ping a R1 1.20 IPV4 e IPV6 desde PC-B escenario 2 
		IPv6	2001:db8:acad:a::1	
	R1, G0/0/1.30	IPv4	10.1.8.65	Figura 25. Ping a R1 1.30 IPV4 e IPV6 desde PC-B escenario 2 
		IPv6	2001:db8:acad:b::1	
	R1, G0/0/1.40	IPv4	10.1.8.97	Figura 26. Ping a R1 1.40 IPV4 e IPV6 desde PC-B escenario 2
		IPv6	2001:db8:acad:c::1	

				
	S1, VLAN 4	IPv4	10.1.8.98	Figura 27. Ping a S1 IPV4 desde PC-B escenario 2 
		IPv6	2001:db8:acad:c::98	Si registramos el siguiente comando IPv6 route ::/0 2001:db8:acad:c::1 para habilitar la PE de IPV6 habrá respuesta, más sin embargo perderá conectividad PE de IPV4 Figura 28. Ping a S1 IPV6 desde PC-B escenario 2 

	S2, VLAN 4	IPv4	10.1.8.99	Figura 29. Ping a S2 IPV4 desde PC-B escenario 2 
		IPv6	2001:db8:acad:c::99	Si registramos el siguiente comando IPv6 route ::/0 2001:db8:acad:c::1 para habilitar la PE de IPV6 habrá respuesta, más sin embargo perderá conectividad PE de IPV4 Figura 30. Ping a S2 IPV6 desde PC-B escenario 2 

CONCLUSIONES

Para el direccionamiento de una LAN pequeña (escenario 1), utilizamos IPV4, donde podemos volverla aún más pequeñas gracias al Subneteo, para ese proceso utilizamos una serie de fórmulas, donde divide las redes físicas a redes lógicas no perdiendo la pertenencia de un dominio, donde permite la organización de subredes

Además, no hubo necesidad de un servidor DHCP en esta red, porque son pocos dispositivos, pocos hosts y es más viable configurar estático (configuración manual) para un mayor control de nuestras direcciones IP

En el escenario 2, El Router y los Switches (capa 3) se configuran para administrarlos de forma segura utilizando el enrutamiento de VLAN, DHCP, Etherchannel y port-security, siendo medidas de control estables que permiten o niegan el acceso a recursos específicos.

La mayor parte de configuraciones de los dispositivos por comandos se llevó por consola ya que es más fiable (seguro) y además se configura procesos que no encontramos en la parte gráficas.

BIBLIOGRAFÍA

Cisco, Networking Academy. Diplomado de Profundización Cisco: Conectividad de red básica y comunicaciones. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010184

Cisco, Networking Academy. Diplomado de Profundización Cisco: Conceptos de Ethernet. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010192

Cisco, Networking Academy. Diplomado de Profundización Cisco: Comunicación entre redes. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010200

Cisco, Networking Academy. Diplomado de Profundización Cisco: Direccionamiento IP. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010208

Cisco, Networking Academy. Diplomado de Profundización Cisco: Comunicaciones de aplicaciones de red. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010216

Cisco, Networking Academy. Diplomado de Profundización Cisco: Crear y asegurar una red pequeña. {En línea}. {24 agosto 2022}. Disponible en: https://lms.netacad.com/mod/lti/view.php?id=55010224

Cisco, Networking Academy. Diplomado de Profundización Cisco: Conceptos de Switching, VLANs y enrutamiento entre redes VLAN. {En línea}. {18 octubre 2022}. https://lms.netacad.com/mod/lti/view.php?id=60748106

Cisco, Networking Academy. Diplomado de Profundización Cisco: Redes Redundantes. {En línea}. {18 octubre 2022}. https://lms.netacad.com/mod/lti/view.php?id=60748114

Cisco, Networking Academy. Diplomado de Profundización Cisco: Redes Disponibles y Confiables. {En línea}. {18 octubre 2022}. https://lms.netacad.com/mod/lti/view.php?id=60748122

Cisco, Networking Academy. Diplomado de Profundización Cisco: Seguridad de L2 y WLAN. {En línea}. {18 octubre 2022}. https://lms.netacad.com/mod/lti/view.php?id=60748130

Cisco, Networking Academy. Diplomado de Profundización Cisco: Conceptos de enrutamiento y configuración. {En línea}. {18 octubre 2022}. https://lms.netacad.com/mod/lti/view.php?id=60748138

ANEXOS

Anexo A. Link de descarga escenario 1 y 2, archivos simulados ptk
https://drive.google.com/drive/folders/1PE5SXVakm9D2VNP_Zw9JuV7FA-27_f8c?usp=sharing