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

JESUS EDUARDO MUÑOZ OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
POPAYÁN
2022

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

JESUS EDUARDO MUÑOZ OROZCO

Diplomado de opción de grado presentado para optar el título de ingeniero de sistemas

Directora: Paulita Flor Salazar

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
POPAYÁN
2022

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Popayán, 27 de noviembre de 2022

AGRADECIMIENTOS

Primero quiero agradecer a Dios que es el camino que nos ilumina todos los días y hace posible que alcancemos todos nuestros logros, a mi familia que es el pilar de todo lo que hago en mi vida y a todas las personas cercanas a mí que de algún modo u han hecho posible este gran logro.

Por ultimo quiero agradecer a la Universidad Nacional Abierta y A Distancia UNAD al personal administrativo y a todos los docentes que hicieron parte de vida en la academia por haberme dado los conocimientos necesarios para afrontar mi vida personal y profesional dándome otorgándome el grado en Ingeniería de sistemas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Router: Conectan redes entre si y múltiples dispositivos a Internet. Analizan los datos que se envían a través de una red, elige la mejor ruta para que se desplacen los datos y los envía en su camino. Protegen la información de las amenazas de seguridad e incluso deciden qué equipos de cómputo tienen prioridad sobre otros.[1]

LAN: Una Local Area Network (por sus siglas) o Red de Área Local, conecta equipos informáticos ubicados en un área geográfica reducida, como un edificio o una habitación.[2]

WAN: Una Wide Area Network (por sus siglas) o Red de Área Amplia, es un conjunto de redes LAN que conecta equipos informáticos que se encuentran en diferentes ubicaciones físicas.[3]

Switch: Los switches o conmutadores permiten que los dispositivos en su red se comuniquen entre sí, recibiendo paquetes de datos y direccionándolos al destinatario correcto. Al hacer posible que la información y los recursos sean compartidos, los switches le ayudan a ahorrar dinero e incrementar la productividad. [4]

DHCP: El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.[5]

[1] CISCO, 2019. Conceptos sobre redes de datos (2019)
[2] CISCO, 2019. Conceptos sobre redes de datos (2019)
[3] CISCO, 2019. Conceptos sobre redes de datos (2019)
[4] CISCO, 2019. Conceptos sobre redes de datos (2019)
[5] MICROSOFT. Protocolo de configuración dinámica de host (DHCP) (2022)

Vlan: Las VLAN se crean en la Capa 2 para reducir o eliminar el tráfico de difusión. Las VLAN son la forma en que divide la red en redes más pequeñas, de modo que los dispositivos y las personas dentro de una sola VLAN se comunican entre sí y no tienen que administrar el tráfico de otras redes.[6]

[6] CISCO, NETCAD Bienvenido a las VLAN (2022)

RESUMEN

En el siguiente documento a modo de informe se quieren mostrar los conocimientos adquiridos en el curso de CISCO diseño e implementación de soluciones integradas LAN/WAN el cual nos posibilita en un fututo acceder a una certificación CCNA (Cisco Certified Network Associate) que es un estándar de calidad en el rubro de las comunicaciones y la tecnología de la información. Cisco nos proporciona el simulador Packet Tracer en donde se pueden diseñar y simular redes de comunicación por medio del cableado adecuado y conexión de diferentes dispositivos electrónicos, así como su configuración por medio de comandos que permiten el enrutamiento de los paquetes de protocolos ipv4 e ipv6 y de esta manera se conmutan las señales enviadas a modo de prueba de manera correcta desde su origen hasta el destino requerido.

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

ABSTRACT

In the following document, as a report, we want to show the knowledge acquired in the CISCO course Design and Implementation of Integrated LAN/WAN Solutions, which enables us in the future to access a CCNA (Cisco Certified Network Associate) certification, which is a standard quality in the field of communications and information technology. Cisco provides us with the Packet Tracer simulator where communication networks can be designed and simulated through the correct wiring and connection of different electronic devices, as well as their configuration through commands that allow the routing of ipv4 and ipv6 protocol packets and in this way, the signals sent to test mode are switched correctly from their origin to the required destination.

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

INTRODUCCIÓN

En el diplomado CISCO de diseño e implementación de soluciones integradas LAN/WAN se desarrolló un plan de capacitación para los estudiantes de la Universidad Nacional Abierta y a Distancia UNAD en infraestructura de redes informáticas e internet, el cual proporcionó a los participantes habilidades y conocimientos de diseño, configuración e implementación de redes y que por medio de la simulación de escenarios didácticos en el simulador Packet Tracer y plataforma CISCO NetAcad se pusieron en práctica y se afianzaron dichas competencias.

Para la práctica final del diplomado se tienen dos escenarios para trabajar tipologías en las que vamos a aplicar los conocimientos aprendidos. En el primer escenario tenemos una topología de red pequeña que se compone de un router, un switch y dos computadores. Se harán las configuraciones pertinentes de dispositivos por protocolos IPV4, creación de red VLAN en switch y el subneting de dos subredes para lograr conexión entre todos los elementos.

En el segundo escenario se requiere conectar una red compuesta por dos computadores y un router que proveerá con conexión DHCP a dichos equipos de cómputo, en los dos switches que tenemos se crea un grupo de puertos EtherChannel con protocolo LACP para hacer comunicación y se crean las VLANS y los puertos trunk necesarios para luego de hacer las configuraciones pertinentes hacer contacto entre dispositivos con las direcciones IPV4 predeterminadas.

1. DESARROLLO DE ESCENARIO 1

Topología dada

Topología del escenario 1

Figura 1. Topología del escenario 1

Fuente: Prueba de habilidades diplomado CCNA

1.1 Parte 1: Construya la Red

Se construye la red teniendo en cuenta las directrices de la topología dada.

Figura 2. Construcción de escenario 1 en simulador

Fuente: Autor

1.2 Parte 2: Desarrolle el esquema de direccionamiento IP

Para este primer escenario debemos configurar los dispositivos de una red pequeña en la que se nos dan un router, un switch y dos computadores, se requiere plantear para cada LAN dada el esquema de direccionamiento IPv4 y que está compuesta por dos subredes a las cuales a partir del espacio de red disponible se les hará subnetting para cumplir con el requerimiento para la LAN1 (60 host) y la LAN2 (20 hosts).

Se tomará el espacio de red disponible de direccionamiento 172.25.3.0. y se hace calculan las sub redes teniendo en cuenta la tabla de direccionamiento.

Tabla de direccionamiento

Tabla 1. Tabla de Direccionamiento

Ítem	Requerimiento
Dirección de Red	172.25.3.0
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1: 172.25.3.62
R1 G0/0/0	Última dirección de host de la subred LAN2: 172.25.3.94
S1 SVI	Segunda dirección de host de la subred LAN1: 172.25.3.2
PC-A	Décima dirección de host de la subred LAN1: 172.25.3.10
PC-B	Décima dirección de host de la subred LAN2: 172.25.3.74

Fuente: Prueba de habilidades diplomado CCNA

1.3 Parte 3: Configure aspectos básicos

Los dispositivos de red Router 1 y switch 1 se configuran mediante conexión de consola y con las líneas de comandos teniendo en cuenta la tabla 2.

1.3.1 Paso 1: Configurar los ajustes básicos

Para configurar el router utilizamos los comandos mostrados a continuación (Tabla 2).

Tabla 2. Configuración de ajustes básicos

TAREAS	ESPECIFICACIÓNES/PROCESOS
Esta configuración DNS viene por defecto y por ello	Router>enable Router#config terminal Router(config)#no ip domain-lookup

TAREAS	ESPECIFICACIÓNES/PROCESOS
se desactiva de la siguiente manera.	
Nombramos el router a (R1) con el siguiente comando	Router(config)#hostname R1
Asignamos el dominio ccna-sa.com con el siguiente comando	R1(config)#ip domain-name ccna-sa.com
Asignamos la contraseña cifrada para el modo EXEC privilegiado (ciscoenpass) con el siguiente comando	R1(config) #enable secret ciscoenpass
Asignamos la contraseña de acceso a la consola (ciscoconpass) y la damos de alta con login.	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecemos la longitud mínima para las contraseñas a 10 caracteres	R1(config)#security passwords min-length 10
Se crea un usuario administrativo para la base de datos local con las siguientes credenciales. Nombre de usuario: admin Password: admin1pass	R1(config)#username admin password admin1pass
Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y damos de alta con login local.	R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit

TAREAS	ESPECIFICACIÓNES/PROCESOS
Se configuran las líneas VTY para que solo acepten protocolos SSH.	R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Se cifran las contraseñas de texto no cifrado con el siguiente comando.	R1(config)#service password-encryption
Configuramos un MOTD Banner el nombre del dispositivo, nombre completo del estudiante y el programa académico al que pertenece.	R1(config)#banner motd #ROUTER R1 JESUS MUNOZ INGENIERIA DE SISTEMAS!#
Se configura la interfaz de G0/0/0 en la que establecemos la descripción, dirección IPv4	R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 172.25.3.94 255.255.255.224 R1(config-if)#description configuracion LAN 2 R1(config-if)#no shutdown
Se configura la interfaz de G0/0/1 en la que establecemos la descripción, dirección IPv4	R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#ip address 172.25.3.62 255.255.255.192 R1(config-if)#description configuracion LAN 1 R1(config-if)#no shutdown

TAREAS	ESPECIFICACIÓNES/PROCESOS
Generamos una clave de cifrado RSA en la cual el modulo contenga un tamaño de 1024 bits	R1(config)#no ip domain-lookup 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]

Fuente: Autor

1.3.2 Paso 2. Configuración del switch

TAREAS	ESPECIFICACIÓNES/PROCESOS
Esta configuración DNS viene por defecto y por ello se desactiva de la siguiente manera.	Switch(config)#no ip domain-lookup
Nombramos el router a (R1) con el siguiente comando	Switch(config)#hostname S1
Asignamos el dominio ccna-sa.com con el siguiente comando	S1(config)#ip domain-name ccna-sa.com
Asignamos la contraseña cifrada para el modo EXEC privilegiado (ciscoenpass) con el siguiente comando	S1(config) #enable secret ciscoenpass
Asignamos la contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass

TAREAS	ESPECIFICACIÓNES/PROCESOS
(ciscoconpass) y la damos de alta con login.	
Apagar todos los puertos sin usar F0/1-4, F0/7-24, G0/1-2	S1(config)#interface range F0/1-4, F0/7-24, G0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit
Se crea un usuario administrativo para la base de datos local con las siguientes credenciales. Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass
Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y damos de alta con login local.	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Se configuran las líneas VTY para que solo acepten protocolos SSH.	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Se cifran las contraseñas de texto no cifrado con el siguiente comando.	S1(config)#service password-encryption
Configuramos un MOTD Banner el nombre del dispositivo, nombre completo del estudiante y el programa académico al que pertenece.	S1(config)#banner motd #ROUTER S1 JESUS MUNOZ INGENIERIA DE SISTEMAS!#

TAREAS	ESPECIFICACIÓNES/PROCESOS
Generamos una clave de cifrado RSA en la cual el modulo contenga un tamaño de 1024 bits	S1(config)#no ip domain-lookup 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]
Se configura la interfaz de administración (SVI) para VLAN1	S1(config)#interface vlan 1 S1(config-if)#description VLAN1 S1(config-if)#ip address 172.25.3.2 255.255.255.192 S1(config-if)#no shutdown Asignamos la puerta enlace S1>enable S1#configure terminal S1(config)#ip default-gateway 172.25.3.62

Fuente: Autor

1.3.3 Paso 3. Configuración de equipos

Teniendo en cuenta la tabla de direccionamiento (tabla 1) se configuran los equipos host PC-A y PC-B

Tabla 3. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000B.BEB6.2D81
Dirección IPv4	172.25.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.25.3.62

Fuente: Elaboración Propia

Tabla 4. Configuración de red de PC-B

Configuración de red de PC-B	
Descripción	**PC-B**
Dirección física	0060.7076.A5B2
Dirección IPv4	172.25.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.25.3.94

Fuente: Elaboración Propia

1.4 Parte 4: Probar y verificar la conectividad de extremo a extremo

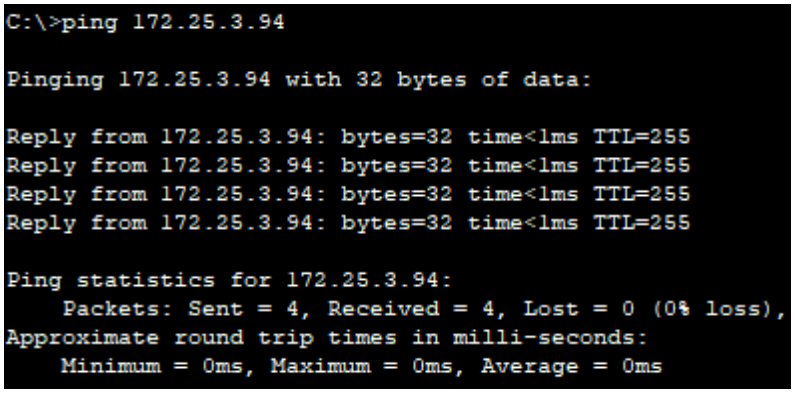
Para probar las conexiones entre dispositivos utilizamos el comando ping y luego ingresamos la dirección ip a la que se quiere enviar paquetes para esto tener en cuenta la tabla 5.

Tabla 5.Tabla de verificación metódica de la conectividad con cada dispositivo de red

Desde	**A**	**Dirección IP**	**Resultados de ping**
PC-A	R1 G0/0/0	172.25.3.94	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 3
	R1 G0/0/1	172.25.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 4
	S1 VLAN 1	172.25.3.2	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 5
	PC-B	172.25.3.74	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 6
PC-B	R1 G0/0/0	172.25.3.94	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 7
	R1 G0/0/1	172.25.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 8
	S1 VLAN1	172.25.3.2	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Exitoso - Figura 9

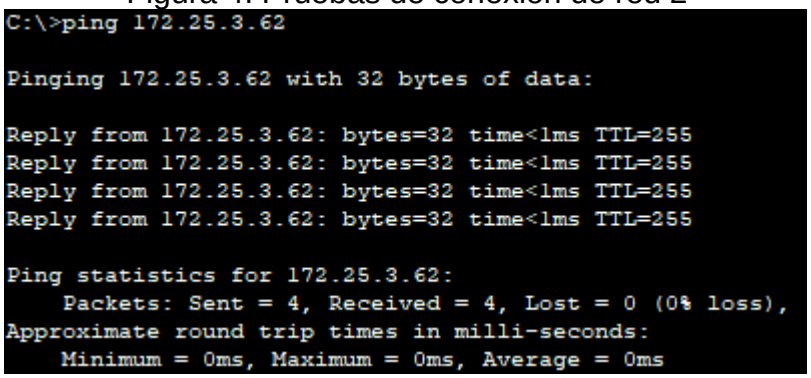
Fuente: Autor

Figura 3. Pruebas de conexión de red 1



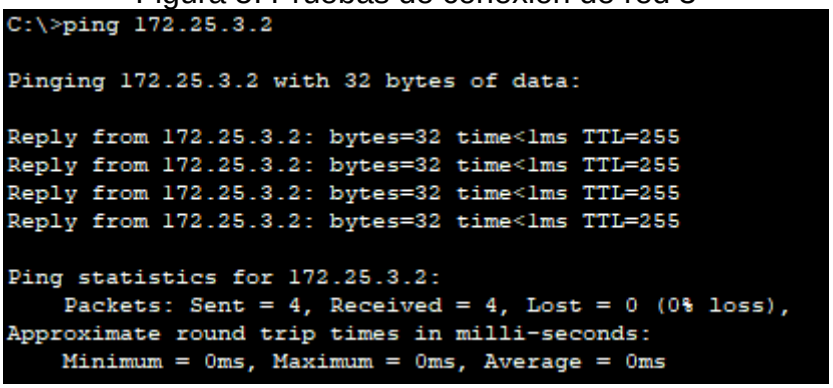
Fuente: Autor

Figura 4. Pruebas de conexión de red 2



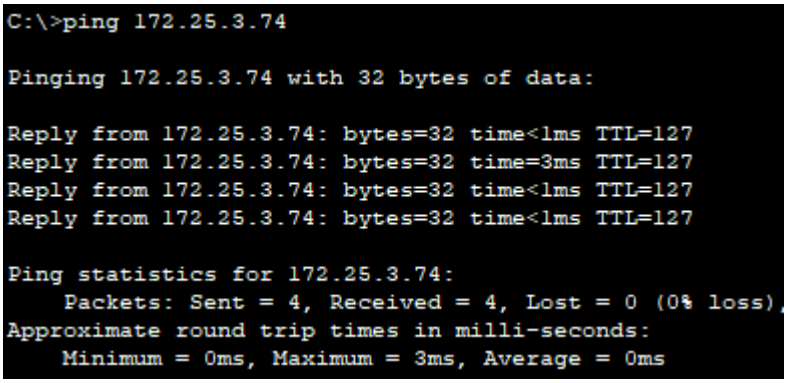
Fuente: Autor

Figura 5. Pruebas de conexión de red 3



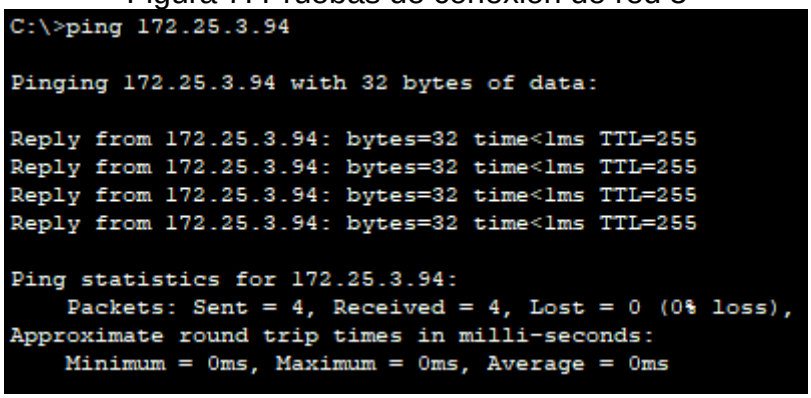
Fuente: Autor

Figura 6. Pruebas de conexión de red 4



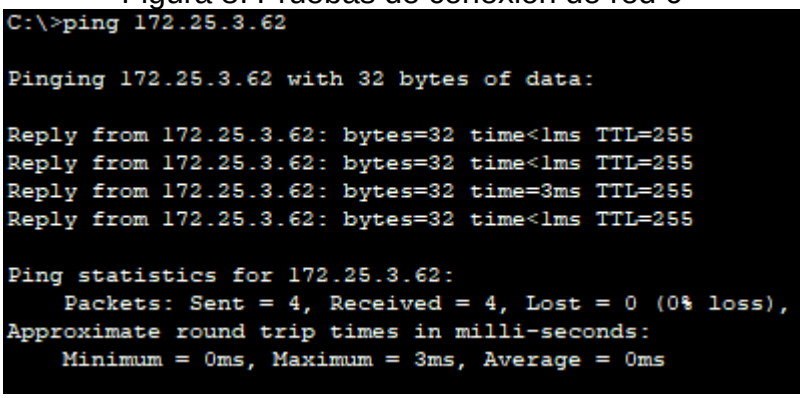
Fuente: Autor

Figura 7. Pruebas de conexión de red 5



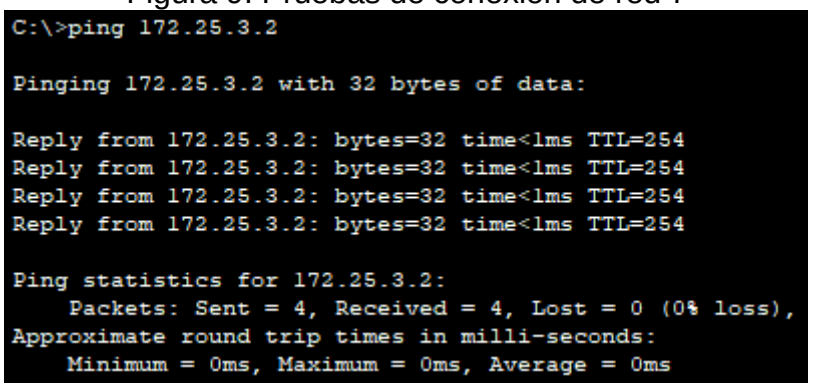
Fuente: Autor

Figura 8. Pruebas de conexión de red 6



Fuente: Autor

Figura 9. Pruebas de conexión de red 7



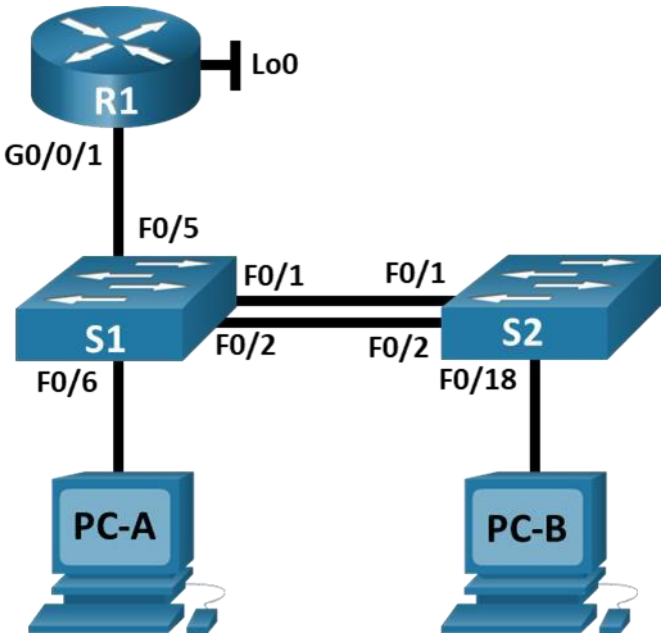
Fuente: Autor

Al hacerse las pruebas se observa que todas resultaron exitosas lo que nos da entender que el subnetting está correcto ya que todas direcciones pertenecen al mismo espacio de red disponible de direccionamiento que se tuvo en cuenta al inicio del ejercicio, además el router y switch se configuraron con los datos resultantes y no presentaron fallas, gracias a esto los dispositivos lograron enviar paquetes entre sí.

2. ESCENARIO 2

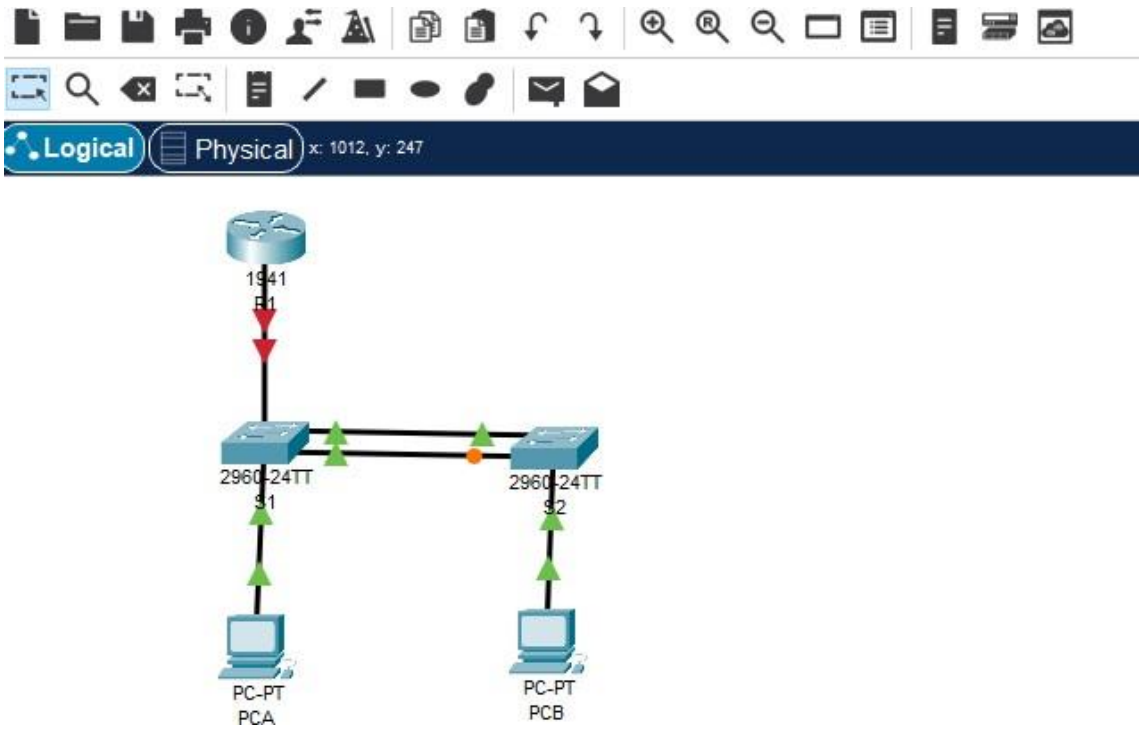
2.1 Topología

Figura 10. Tipología escenario 2



Fuente: Prueba de habilidades practica CCNA - UNAD

Figura 11. Construcción de la red



Fuente: Autor

En este escenario se requiere configurar una red compuesta por un router, un switch y dos computadores que admitan tanto IPv4 como IPv6 para los hosts soportados aceptando protocolo DHCP. Se hará configuración de equipos con enrutamiento de las VlLAN, conexión entre switches por medio de Etherchannel y apertura de puertas por medio de enlaces truncales. Las conexiones se hacen de manera segura.

Tabla de VLAN

Tabla 6. Tabla de VLAN

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

Fuente: Prueba de habilidades practica CCNA - UNAD

Tabla de asignación de direcciones

Tabla 7. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.25.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.25.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.25.8.97 /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	10.25.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.25.8.99 /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

Fuente: Prueba de habilidades practica CCNA - UNAD

2.2 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

Para borrar las configuraciones de inicio y las VLAN del router y del switch, ejecutamos el comando erase startup-config y para volver a cargar los dispositivos hacemos reload. Las VLAN se reinician con el comando delete vlan.dat pero no arrojan ningún resultado.

ROUTER

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#show startup-config
startup-config is not present
Router#reload
Proceed with reload? [confirm]

SWITCH 1 Y SWITCH 2

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#show startup-config
startup-config is not present
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.

Se ejecuta el comando sdm prefer dual-ipv4-and-ipv6 default y le damos reload.

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#
%SYS-5-CONFIG_I: Configured from console by console
Switch#reload
System configuration has been modified. Save? [yes/no]:
% Please answer 'yes' or 'no'.
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]

2.2.2 Paso 2: Configurar R1

Configuramos el router con las siguientes instrucciones teniendo en cuenta la tabla de asignación de direcciones (Tabla 7).

Tabla 8. Configuración inicial R1

Tarea	Especificación
Desactivamos la configuración DNS, esta viene por defecto y por ello se desactiva de la siguiente manera.	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombramos el router a (R1) con el siguiente comando	Router(config)#hostname R1
Asignamos el dominio con el siguiente comando (ccna-sa.com)	R1(config)#ip domain-name ccna-sa.com
Asignamos la contraseña cifrada para el modo EXEC privilegiado (class) con el siguiente comando	R1(config)#enable password class
Asignamos la contraseña de acceso a la consola (cisco) y la damos de alta con login.	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Establecemos la longitud mínima para las contraseñas a 5 caracteres	R1(config)#security passwords min-length 5
Se crea un usuario administrativo para la base de datos local con las siguientes credenciales.	R1(config)#username admin password admin1pass

Tarea	Especificación
Nombre de usuario: admin Password: admin1pass	
Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y damos de alta con login local.	R1(config)# line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Se configuran las líneas VTY para que solo acepten protocolos SSH.	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Se cifran las contraseñas de texto no cifrado con el siguiente comando.	R1(config)#service password-encryption
Configuramos un MOTD Banner el nombre del dispositivo, nombre completo del estudiante y el programa académico al que pertenece.	R1(config)#banner motd #ROUTER R1 JESUS MUNOZ INGENIERIA DE SISTEMAS!#
Para Habilitar el routing IPv6 se utiliza el siguiente comando.	R1(config)#ipv6 unicast-routing
Se configura la interfaz de G0/0/1 y las subinterfaces en las que establecemos la descripción, dirección IPv4. Así como también establecemos la dirección IPv6 y la dirección local de enlace IPv6 como fe80: :1	R1(config)#interface g0/0/1 R1(config-if)#interface g0/0/1.20 R1(config-subif)#description VLAN 20 Docentes R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#ip add 10.25.8.1 255.255.255.192 R1(config-subif)#ipv6 add fe80::98 link-local

Tarea	Especificación
(ver tabla de asignación de direcciones)	R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.30 R1(config-subif)#description VLAN 30 Estudiantes R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#ip add 10.25.8.65 255.255.255.224 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#no shutdown R1(config-if)#interface g0/0/1.40 R1(config-subif)#description VLAN 40 INVITADOS R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#ip add 10.25.8.97 255.255.255.248 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#no shut R1(config-subif)#interface g0/0/1.56 R1(config-subif)#encapsulation dot1q 56 R1(config-subif)#no shutdown
Configuramos la interface lógica Loopback0 estableciendo la descripción,	R1(config)#inter loopback 0 R1(config-if)#ip add 209.165.201.1 255.255.255.224

Tarea	Especificación
dirección IPv4 y la dirección local de enlace IPv6 como fe80::1 (Tabla 7)	R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add fe80::1 link-local R1(config-if)#no shutdown
Generamos una clave de cifrado RSA en la cual el modulo contenga un tamaño de 1024 bits	R1(config)#crypto key generate rsa

Fuente: Elaboración Propia

2.2.3 Paso 3: Configure S1 y S2.

Configure S1

Configuramos el SWITCH 1 con las siguientes instrucciones teniendo en cuenta la tabla de asignación de direcciones (Tabla 7).

Tabla 9. Configuración inicial switch 1

Tarea	Especificación
Desactivamos la configuración DNS, esta viene por defecto y por ello se desactiva de la siguiente manera.	S1 (config)#no ip domain lookup
Nombramos el switch (S1) con el siguiente comando	S1(config)#hostname S1
Asignamos el dominio con el siguiente comando (ccna-sa.com)	S1(config)#ip domain-name ccna-sa.com
Asignamos la contraseña cifrada para el modo EXEC privilegiado (class) con el siguiente comando	S1(config)#enable secret class S1(config)#service password-encryption
Asignamos la contraseña de acceso a la consola (cisco) y la damos de alta con login.	S1(config)#line console 0 S1(config-line)#password cisco

Tarea	Especificación
	S1(config-line)#login S1(config-line)#exit
Se crea un usuario administrativo para la base de datos local con las siguientes credenciales. Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass
Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y damos de alta con login local.	S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Se configuran las líneas VTY para que solo acepten protocolos SSH.	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Se cifran las contraseñas de texto no cifrado con el siguiente comando	S1(config)#service password-encryption
Configuramos un MOTD Banner el nombre del dispositivo, nombre completo del estudiante y el programa académico al que pertenece.	S1(config)#banner motd #ROUTER S1 JESUS MUNOZ INGENIERIA DE SISTEMAS!#
Generamos una clave de cifrado RSA en la cual el modulo contenga un tamaño de 1024 bits	S1(config)#crypto key generate rsa S1(config)#exit

Tarea	Especificación
Se configura para S1 la interfaz de administración (SVI) VLAN 40, asignamos la dirección IPv4 de capa 3 y la dirección local de enlace IPv6 como **FE80: :98,** todo esto teniendo en cuenta la tabla 7.	S1(config)#interface vlan 40 S1(config-if)#ip address 10.25.8.98 255.255.255.248 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ip default-gateway 10.25.8.97
Configuración la puerta de enlace predeterminada con la dirección 10.25.8.97 para IPv4	S1(config)#ip default-gateway 10.25.8.97

Fuente: Elaboración Propia

Configure S2.

Configuramos el SWITCH 2 con las siguientes instrucciones teniendo en cuenta la tabla de asignación de direcciones (Tabla 7).

Tabla 10. Configuración inicial switch 2

Tarea	Especificación
Desactivamos la configuración DNS, esta viene por defecto y por ello se desactiva de la siguiente manera.	Switch(config)#no ip domain lookup
Nombramos el switch (S1) con el siguiente comando	Switch(config)#hostname S2
Asignamos el dominio con el siguiente comando (ccna-sa.com)	S2(config)#ip domain-name ccna-sa.com
Asignamos la contraseña cifrada para el modo EXEC privilegiado (class) con el siguiente comando	S2(config)#enable secret class

Tarea	Especificación
Asignamos la contraseña de acceso a la consola (cisco) y la damos de alta con login.	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit
Se crea un usuario administrativo para la base de datos local con las siguientes credenciales. Nombre de usuario: admin Password: admin1pass	S2(config)#username admin password admin1pass
Configuramos el inicio de sesión en las líneas VTY para que use la base de datos local y damos de alta con login local.	S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit
Se configuran las líneas VTY para que solo acepten protocolos SSH.	S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Se cifran las contraseñas de texto no cifrado con el siguiente comando	S2(config)#service password-encryption
Configuramos un MOTD Banner el nombre del dispositivo, nombre completo del estudiante y el programa académico al que pertenece.	S2(config)#banner motd #ROUTER S2 JESUS MUNOZ INGENIERIA DE SISTEMAS!#
Generamos una clave de cifrado RSA en la cual el modulo contenga un tamaño de 1024 bits.	S2(config)#crypto key generate rsa

Tarea	Especificación
Se configura para S2 la interfaz de administración (SVI) VLAN 40, asignamos la dirección IPv4 de capa 3 y la dirección local de enlace IPv6 como **FE80: :99,** todo esto teniendo en cuenta la tabla 7.	S2(config)#inter vlan 40 S2(config-if)#ip add 10.25.8.99 255.255.255.248 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#ipv6 add 2001:db8:acad:c::99/64
Configuración la puerta de enlace predeterminada con la dirección 10.25.8.97 para IPv4	S2(config)#ip default-gateway 10.25.8.97

Fuente: Elaboración Propia

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

2.3.1 Paso 4: Configurar S1

Configuramos el Switch 1 con las especificaciones que se muestran a continuación y teniendo en cuenta la tabla de asignación de direcciones (Tabla 7) y la tabla de VLAN (Tabla 6).

Configuración VLAN S1

Tabla 11. Configuración VLAN S1

Tarea	Especificación
Creamos las VLAN con las que se va a trabajar VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S1>enable S1#configure terminal S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit

Tarea	Especificación
	S1(config)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#end
Creamos los enlaces para la trasmisión de trafico de varias VLAN trunk 802.1Q que utilicen la VLAN 56native en las Interfaces F0/1, F0/2 y F0/5	S1(config-if)#interface range f0/1-2, f0/5 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56 S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56
Creamos un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, Usar el protocolo LACP para la negociación de S1 y S2.	S1(config)#interface range f0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config)#interface port-channel 1 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56
Configuramos el puerto de acceso de host para VLAN 20, Interface F0/6	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20
Para la seguridad del anterior puerto se configura para que permita 4 direcciones MAC.	S1(config)#inter f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 4 S1(config-if)#switchport port-security violation

Tarea	Especificación
	shutdown S1(config-if)#switchport port-security mac-address sticky
Por razones de seguridad se asignan a VLAN 50 todas las interfaces no utilizadas y luego se apagan.	S1(config)#interface range g0/1-2, f0/3-4, f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#shutdown S1(config-if-range)#switchport port-security S1(config-if-range)#switchport port-security violation shutdown

Fuente: Elaboración Propia

2.3.2 Paso 5: Configure el S2.

Configuramos el Switch 1 con las especificaciones que se muestran a continuación y teniendo en cuenta la tabla de asignación de direcciones (Tabla 7) y la tabla de VLAN (Tabla 6).

Configuración VLAN S2

Tabla 12. Configuración VLAN S2

Tarea	Especificación
Creamos las VLAN con las que se va a trabajar VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S2>enable S2#configure terminal S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#name Invitados

	S2(config-vlan)#exit S2(config)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56 S1(config-vlan)#name Native S2(config-vlan)#exit S2(config)#end
Creamos los enlaces para la trasmisión de trafico de varias VLAN trunk 802.1Q que utilicen la VLAN 56 native en las Interfaces F0/1 y F0/2.	S2(config)#inter range f0/1-2 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56
Creamos un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, Usar el protocolo LACP para la negociación de S1 y S2.	S2(config)#interface range f0/1-2 S2(config-if-range) #channel-group 1 mode passive S2(config)#interface port-channel 1 S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56
Configuramos el puerto de acceso de host paraVLAN 20, Interface F0/18	S2(config)#inter f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30
Para la seguridad del anterior puerto se configura para que permita 4 direcciones MAC	S2(config)#inter f0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 4

	S2(config-if)#switchport port-security violation shutdown S2(config-if)#switchport port-security mac-address sticky
Por razones de seguridad se asignan a VLAN 50 todas las interfaces no utilizadas y luego se apagan.	S2(config-if)#interface range g0/1-2, f0/3-17, f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#shutdown S2(config-if-range)#switchport port-security S2(config-if-range)#switchport port-security violation shutdown

Fuente: Elaboración Propia

2.4 Parte 3: Configurar soporte de host

2.4.1 Paso 6: Configure R1

Configuramos el Router con las especificaciones que se muestran a continuación y teniendo en cuenta la tabla de asignación de direcciones (Tabla 7) y la tabla de VLAN (Tabla 6).

Configuración de DHCP Router

Tabla 13. Configuración de DHCP Router

Tarea	Especificación
Se configuran los protocolos IPv4 DHCP paraVLAN 20, se hace crando un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred, asignamos	R1(config)#ip dhcp pool vlan_20 R1(dhcp-config)#network 10.25.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.25.8.1 R1(dhcp-config)#domain-name unad-ccna-sa.net

Tarea	Especificación
nombre de dominio unad-ccna-sa.net yestablecemos la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada, de esta forma los equipos de manera automática adquirirán el host.	R1(dhcp-config)#ip dhcp excluded-address 10.25.8.2 10.25.8.52 ip dhcp excluded-address 10.25.8.62
Se configuran los protocolos IPv4 DHCP paraVLAN 30, se hace crando un grupo DHCP para VLAN 30, compuesto por lasúltimas 10 direcciones de la subred, asignamos nombre de dominio unad-ccna-sb.net yestablecemos la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada, de esta forma los equipos de manera automática adquirirán el host.	R1(config)#ip dhcp pool vlan_30 R1(dhcp-config)#network 10.25.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.25.8.65 R1(dhcp-config)#domain-name unad-ccna-sb.net R1(dhcp-config)#ip dhcp excluded-address 10.25.8.65 10.25.8.84

Fuente: Elaboración Propia

2.4.2 Paso 7: 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 14. Configuración de red de PC-A

PC-A	
Descripción	Computador A
Dirección física	0010.1120.5560
Dirección IP	10.25.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.25.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Elaboración Propia

Tabla 15. Configuración de red de PC-B

PC-B	
Descripción	Computador B
Dirección física	00D0.BADA.8549
Dirección IP	10.25.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.25.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Elaboración Propia

2.5 Parte 4: Probar y verificar la conectividad de extremo a extremo

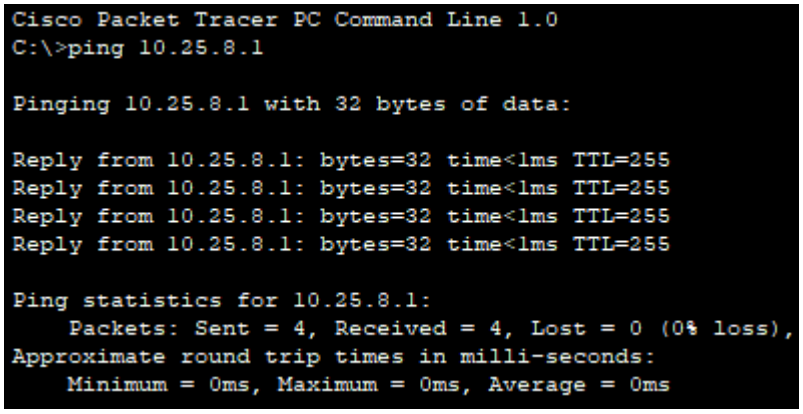
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

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:

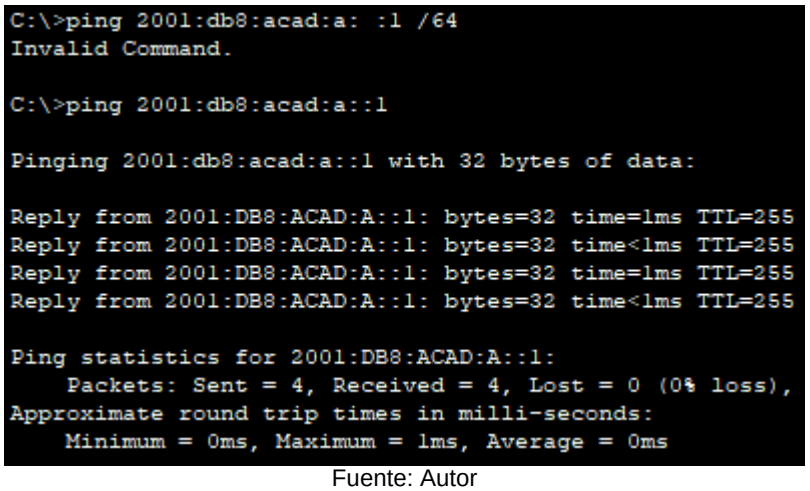
Tabla 16. Pruebas de conectividad

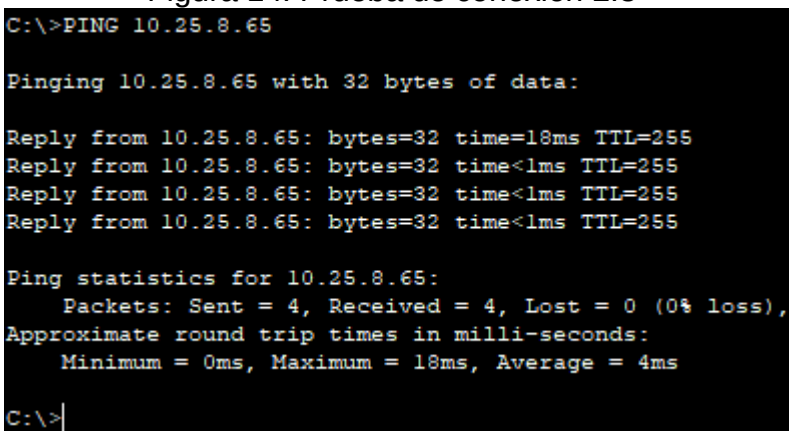
PC -A			
Desde	Dirección IP		Resultados de ping
R1, G0/0/1.20	IPv4	10.25.8.1	PING EXITOSO

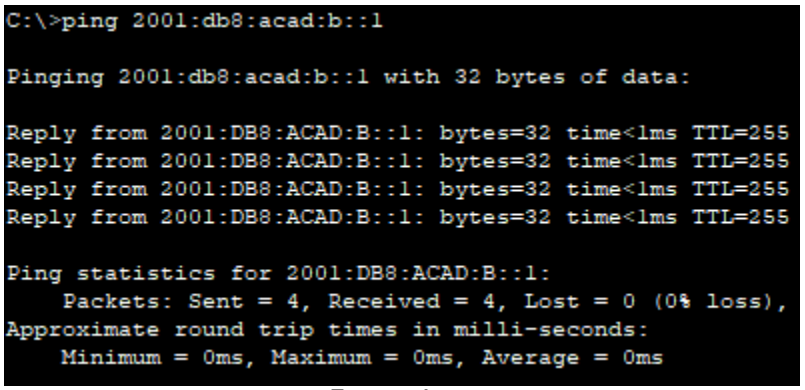
Figura 12. Prueba de conexión 2.1



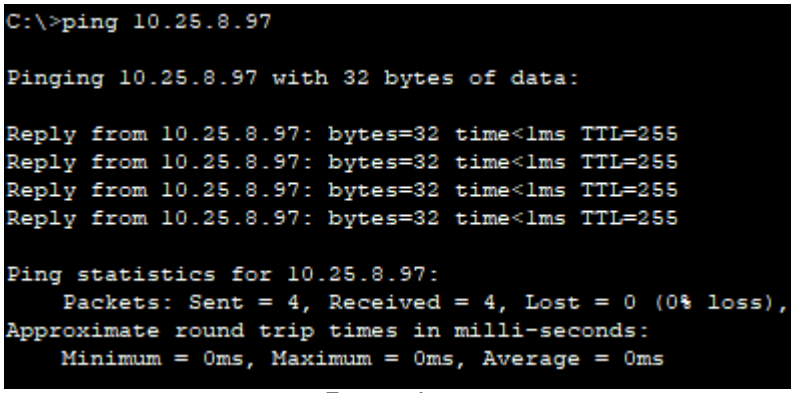
Fuente: Autor

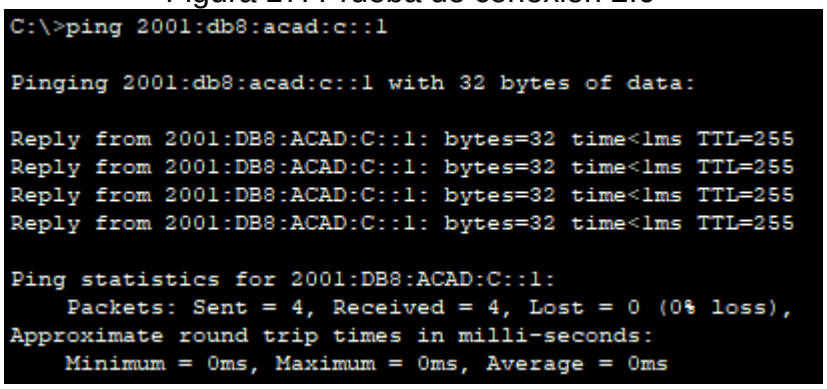
<table>
<tr><td rowspan="2">R1, G0/0/1.20</td><td>IPv6</td><td>2001:db8:acad:a: :1</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 13. Prueba de conexión 2.2
 

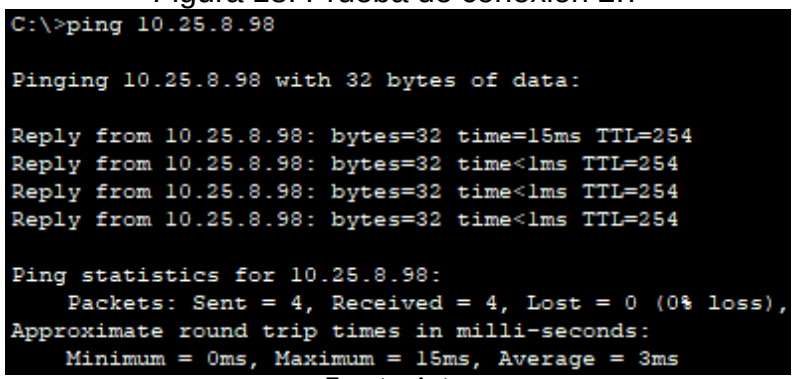
Fuente: Autor</td></tr>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="4">R1, G0/0/1.30</td><td>IPv4</td><td>10.25.8.65</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 14. Prueba de conexión 2.3
 

Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b::1</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 15. Prueba de conexión 2.4
 

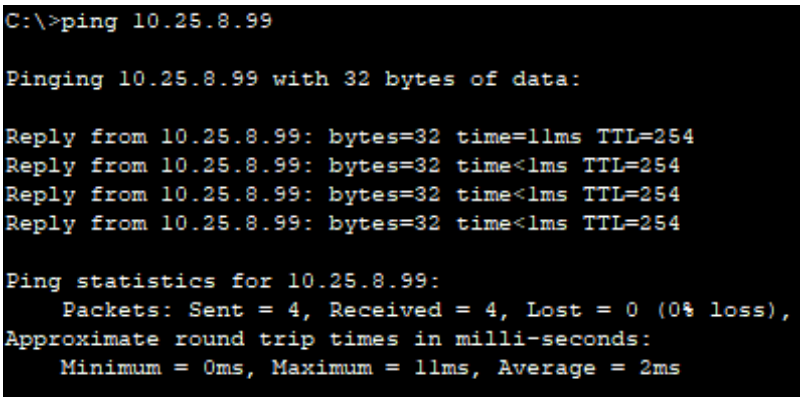
Fuente: Autor</td></tr>
</table>

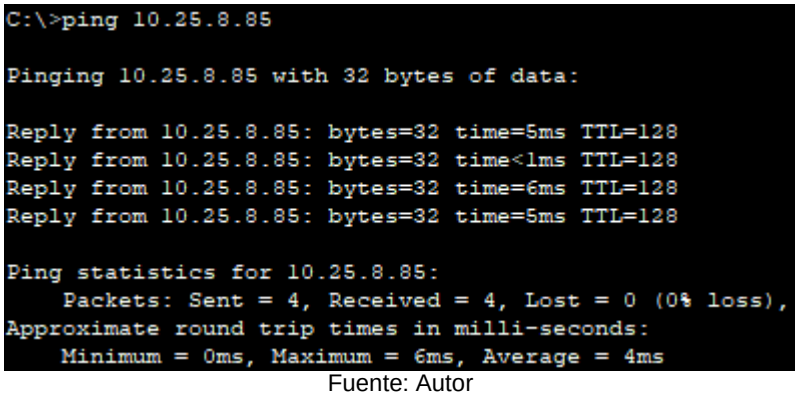
<table>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="4">R1, G0/0/1.40</td><td>IPv4</td><td>10.25.8.97</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 16. Prueba de conexión 2.5
 

Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::1</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 17. Prueba de conexión 2.6
 

Fuente: Autor</td></tr>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="2">S1, VLAN 40</td><td>IPv4</td><td>10.25.8.98</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 18. Prueba de conexión 2.7
 

Fuente: Autor</td></tr>
</table>

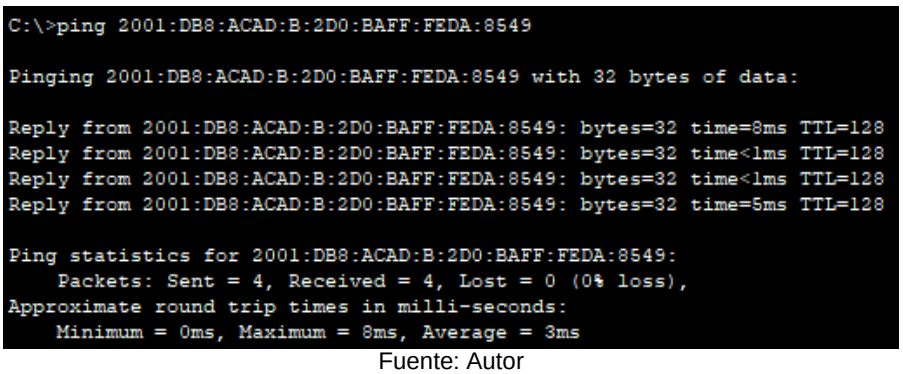
<table>
<tr><td rowspan="2"></td><td>IPv6</td><td>2001:db8:acad:c::98</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">La conexión se realiza de forma correcta pero por falla de plataforma arroja error</td></tr>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="4">S2, VLAN 40</td><td>IPv4</td><td>10.25.8.99</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 19. Prueba de conexión 2.8
 

Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::99</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">La conexión se realiza de forma correcta pero por falla de plataforma arroja error</td></tr>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="3">PC-B</td><td>IPv4</td><td>10.25.8.85</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 20. Prueba de conexión 2.9
 

Fuente: Autor</td></tr>
</table>

	IPv6	2001:DB8:ACAD:B:2D0:BAFF:FEDA:8549	PING EXITOSO

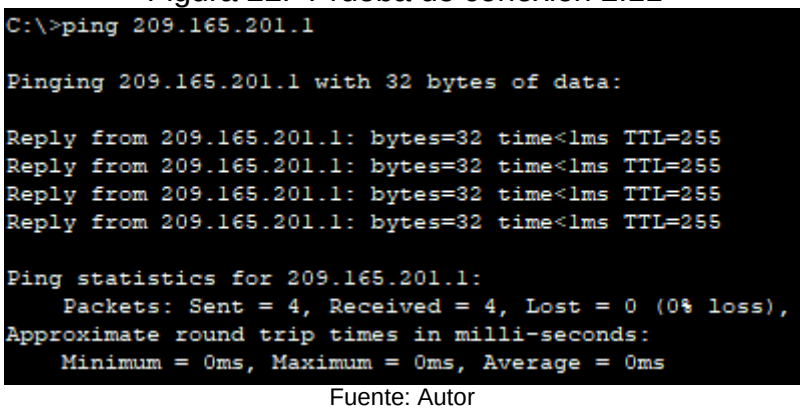
Figura 21. Prueba de conexión 2.10



Fuente: Autor

Desde	Dirección IP		Resultados de ping
R1 Bucle 0	IPv4	209.165.201.1	PING EXITOSO

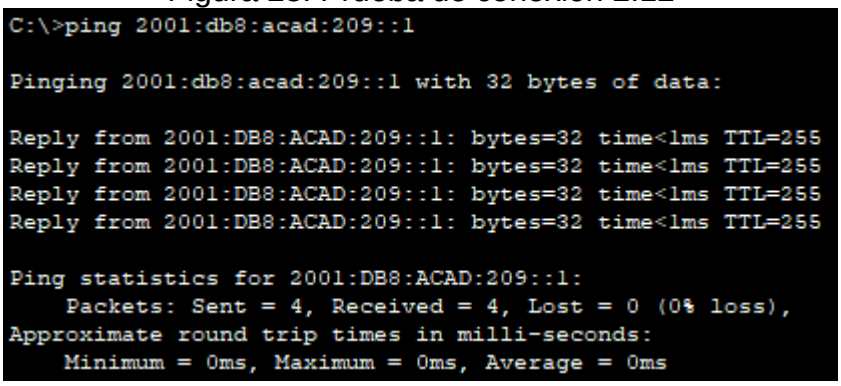
Figura 22. Prueba de conexión 2.11



Fuente: Autor

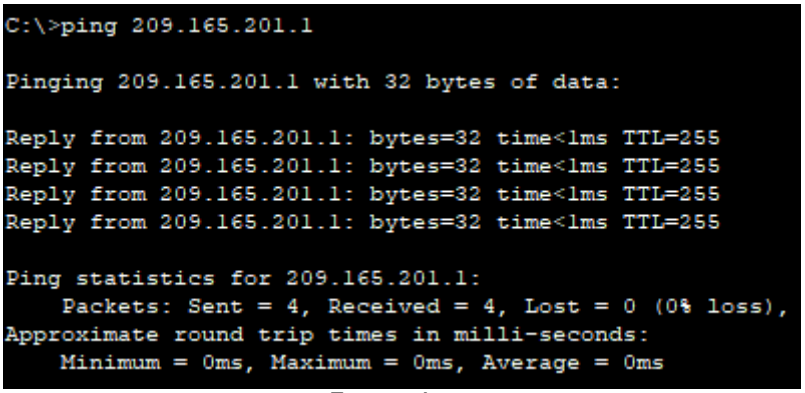
	IPv6	2001:db8:acad:209::1	PING EXITOSO

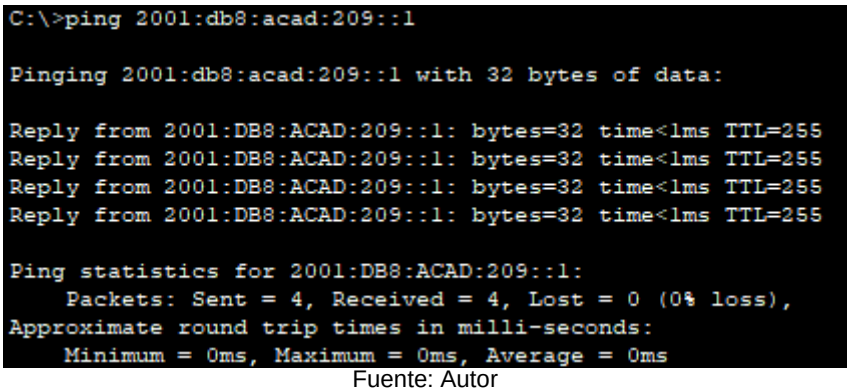
Figura 23. Prueba de conexión 2.12



Fuente: Autor

PC -B

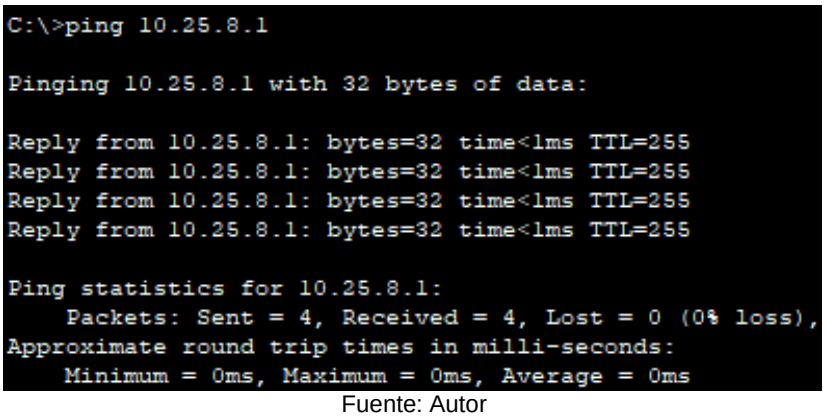
<table>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="4">R1 Bucle 0</td><td>IPv4</td><td>209.165.201.1</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 24. Prueba de conexión 2.13
 

Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:209::1</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 25. Prueba de conexión 2.14
 

Fuente: Autor</td></tr>
</table>

Desde	Dirección IP		Resultados de ping
R1, G0/0/1.20	IPv4	10.25.8.1	PING EXITOSO

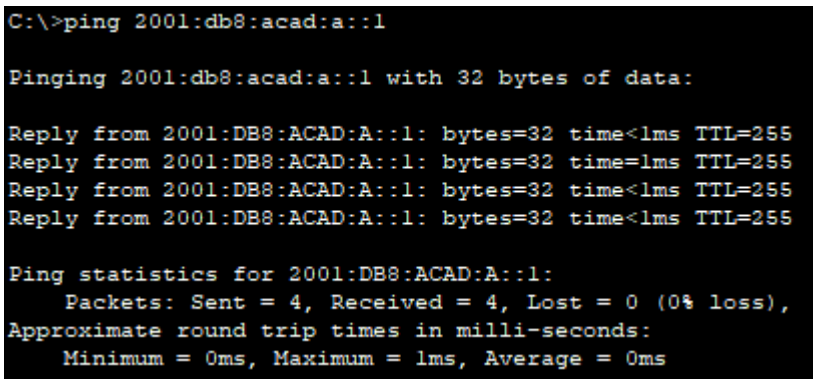
Figura 26. Prueba de conexión 2.15



Fuente: Autor

	IPv6	2001:db8:acad:a: :1	PING EXITOSO

Figura 27. Prueba de conexión 2.16



Fuente: Autor

Desde	Dirección IP		Resultados de ping
R1, G0/0/1.30	IPv4	10.25.8.65	PING EXITOSO

Figura 28. Prueba de conexión 2.17

```
C:\>ping 10.25.8.65

Pinging 10.25.8.65 with 32 bytes of data:

Reply from 10.25.8.65: bytes=32 time<1ms TTL=255
Reply from 10.25.8.65: bytes=32 time<1ms TTL=255
Reply from 10.25.8.65: bytes=32 time<1ms TTL=255
Reply from 10.25.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.25.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

	IPv6	2001:db8:acad:b: :1	PING EXITOSO

Figura 29. Prueba de conexión 2.18

```
C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

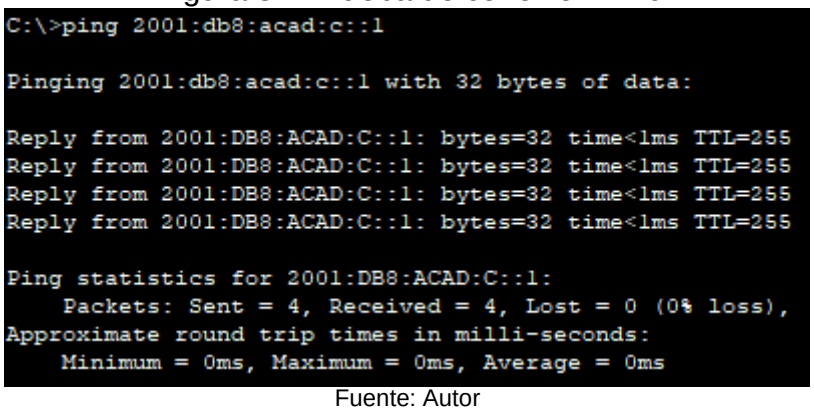
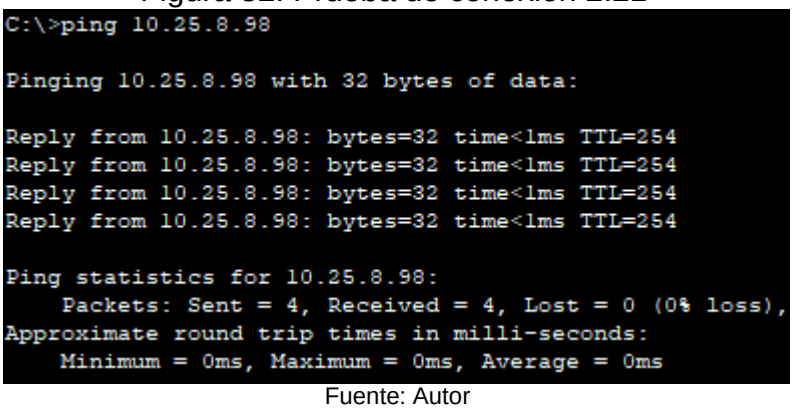
Fuente: Autor

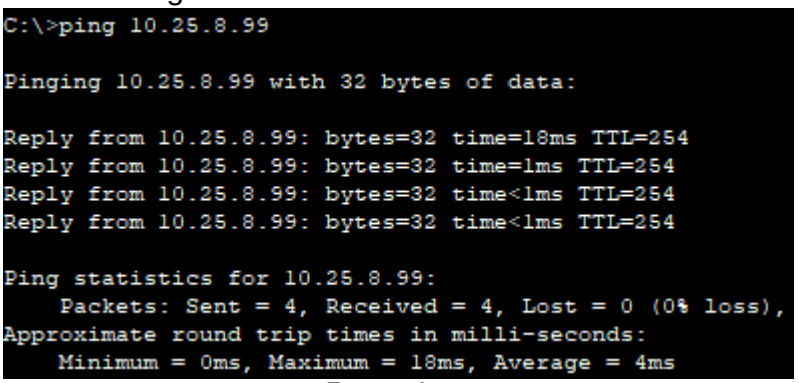
Desde	Dirección IP		Resultados de ping
R1, G0/0/1.40	IPv4	10.25.8.97	PING EXITOSO

Figura 30. Prueba de conexión 2.19

```
C:\>ping 10.25.8.97

Pinging 10.25.8.97 with 32 bytes of data:

Reply from 10.25.8.97: bytes=32 time<1ms TTL=255
Reply from 10.25.8.97: bytes=32 time<1ms TTL=255
Reply from 10.25.8.97: bytes=32 time<1ms TTL=255
Reply from 10.25.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.25.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

	IPv6	2001:db8:acad:c::1	PING EXITOSO
	Figura 31. Prueba de conexión 2.20  Fuente: Autor		
Desde	Dirección IP		Resultados de ping
S1, VLAN 40	IPv4	10.25.8.98	PING EXITOSO
	Figura 32. Prueba de conexión 2.21  Fuente: Autor		
	IPv6	2001:db8:acad:c::98	PING EXITOSO
	La conexión se realiza de forma correcta pero por falla de plataforma arroja error		

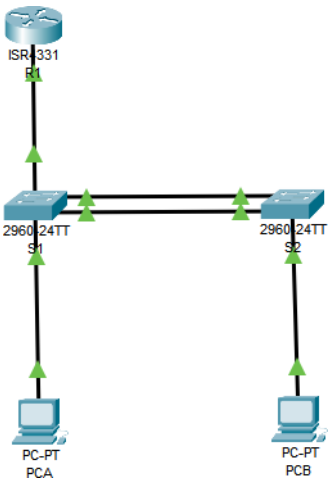
<table>
<tr><td>Desde</td><td colspan="2">Dirección IP</td><td>Resultados de ping</td></tr>
<tr><td rowspan="4">S2, VLAN 40</td><td>IPv4</td><td>10.25.8.99</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">Figura 33. Prueba de conexión 2.22
 

Fuente: Autor</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c: :99</td><td>PING EXITOSO</td></tr>
<tr><td colspan="3">La conexión se realiza de forma correcta pero por falla de plataforma arroja error</td></tr>
</table>

Fuente: Elaboración Propia

Las conexiones resultaron exitosas puesto que se hizo una correcta configuración de las VLAN y los enlaces troncales que hicieron un preciso direccionamiento del tráfico entre dispositivos, también se logró con éxito el puente en los switches por medio del grupo Etherchannel, por último, el router envío de manera correcta los protocolos DHCP puesto que están en el mismo rango de direcciones y puerta de enlace predeterminada.

Figura 34. Red conectada correctamente



Fuente: Autor

CONCLUSIONES

En el desarrollo del escenario uno se trabajó en una red pequeña en la cual a partir de un espacio de red disponible se hizo el cálculo de host para dos subredes, después de esto se configuraron los equipos con sus respectivas direcciones y puertas de enlace por medio de protocolos IPv4 e interface virtual SVI.

En el escenario dos se trabajó una red en la que para lograr conexión entre dispositivos se hicieron configuraciones entre dispositivos por medio de protocolos IPv4 e IPv6 con las direcciones de red dadas, se solucionó el problema de conexión y tráfico entre equipos por medio de interfaces SVI, enlaces troncales y puertos de enlace EtherChannel, además de conexión automática DCHP para los dispositivos finales, al final se solucionó el problema de redundancia.

Tanto el escenario uno como el escenario dos a los dispositivos se les hizo protección por medio de credenciales de usuario y contraseña, también se apagaron todos los puertos sin usar, todo esto para proteger la seguridad de la red.

Se comprobaron las conexiones en los dos escenarios haciendo pruebas de envío de paquetes entre dispositivos las cuales arrojaron mensajes exitosos en la mayoría de las pruebas y se concluyó que debido a un fallo del simulador algunas de estas no tuvieron éxito dejando en claro que estaban correctas las conexiones.

BIBLIOGRAFÍA

CISCO. Configuración básica de switches y terminales. Introducción a las redes {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/2.2.1

CISCO. Configuración básica de un router. Introducción a las redes {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/10.1.1

CISCO. Resolución de dirección. Introducción a las redes {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/9.0.1

CISCO. Asignación de direcciones IPv4. Introducción a las redes {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/11.0.1

CISCO. Asignación de direcciones IPv6. Introducción a las redes {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/12.0.1

CISCO. ICMP. Introducción a las redes. {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/13.0.1

CISCO. Capa de transporte. Introducción a las redes. {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/14.0.1

CISCO. Capa de transporte. Introducción a las redes. {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/15.0.1

CISCO. Fundamentos de seguridad de la red. Introducción a las redes {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/16.0.1

CISCO. Crear una red pequeña. Introducción a las redes {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/itn-dl/17.0.1

CISCO. Configuración básica de dispositivos. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022). Disponible en: https://contenthub.netacad.com/srwe-dl/1.0.1

CISCO. Conceptos de Switching. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/2.0.1

CISCO. VLANs. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/3.0.1

CISCO. Enrutamiento inter VLAN. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/4.0.1

CISCO. STP. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/5.0.1

CISCO. EtherChannel. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/6.0.1

CISCO. DHCPv4. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {26 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/7.0.1

CISCO. SLAAC y conceptos de DHCPv6. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {24 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/8.0.1

CISCO. Conceptos FHRP. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {24 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/9.0.1

CISCO. Conceptos de seguridad en LAN. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/10.0.1

CISCO. Configuración de seguridad en el switch. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {25 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/11.0.1

CISCO. Conceptos WLAN. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/12.0.1

CISCO. Conceptos de enrutamiento. https. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/14.0.1

CISCO. Enrutamiento estático. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/15.0.1

CISCO. Resolución de problemas en rutas estáticas y rutas por defecto. Conmutación, enrutamiento y fundamentos inalámbricos {En línea} (2022) {27 de noviembre 2022}. Disponible en: https://contenthub.netacad.com/srwe-dl/16.0.1

ANEXOS

Anexo A

Link simulación escenario 1 Escenario1_Prueba de habilidades.pkt

Anexo B

Link simulación escenario 2 Escenario2_Prueba de habilidades.pkt