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

GABRIEL EDUARDO VERDUGO MEDINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SANTA MARTA
2022

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

GABRIEL EDUARDO VERDUGO MEDINA

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

Paulita Flor Salazar
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SANTA MARTA
2022

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Santa Marta, 27 de noviembre del 2022

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

SUBNETTING: El subnetting o subneteo, es la técnica de organizar una red con la finalidad de obtener de ella una mejor prestación de servicios. Consiste en dividir una red, sea de clase A, B o C, en dos o más subredes. El número de subredes es siempre un valor 2^n, donde n es el número de bits de la parte del host que se "prestan" a la parte de la red. Si no prestamos ningún bit, sólo tendremos una subred ($2^0 = 1$).[1]

RED DE ÁREA LOCAL LAN: Este tipo de red que tiene como característica una determinada extensión no muy amplia que puede establecerse en un solo edificio o local. Según Stallings (2004): Para las LAN hay muy diversas configuraciones. De entre ellas, Las más habituales son las LAN conmutadas y las LAN inalámbricas. Dentro de las conmutadas, las más populares son las LAN ethernet, constituidas por único conmutador o alternativamente, implementadas mediante un conjunto de conmutadores interconectados entre sí.[2]

VLAN: Las LANs virtuales (VLANs) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre si como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes.[3]

CAPA OSI 3: Proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes, IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red. Otros protocolos de capa de red incluyen protocolos de enrutamiento como Open Shortest Path First (OSPF) y protocolos de mensajería como Internet Control Message Protocol (ICMP). Para lograr comunicaciones end-to-end a través de los límites de la red, los protocolos de capa de red realizan cuatro operaciones básicas (Direccionamiento de dispositivos finales, Encapsulación, Enrutamiento y Desencapsulación).[4]

[1] CRUZ,Wilfredo. Subnetting.
[2] CARRIÓN, Amaya, WENDY Elsa, Redes De Computadoras. (2018).
[3] CASTILLO, Porturas, AUGUSTO Noé, Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabib. (2019).
[4] CISCO, Capa de red.

RESUMEN

Se define la presente prueba de habilidades como un aprendizaje en base a las actividades evaluativas que se dieron en el Diplomado de Profundización CCNA, el cual permitió formarse en base a conceptos, conectividad, protocolos de ethernet en las telecomunicaciones, redes integradas LAN / WAN y las diferentes configuraciones establecidas para los dispositivos incorporados en ella; encontrando diferentes ejercicios de aprendizaje que permiten la solución de problemas diversos a través de los recursos educativos presentados por la universidad y por los diferentes módulos establecidos en Cisco.

De acuerdo con lo anterior, es necesario abordar las diferentes series de temáticas para así poder adquirir los conocimientos necesarios en cuanto a las funcionalidades de los enrutadores y conmutadores, el cual permite crear redes pequeñas y aplicar los diferentes componentes en cuanto a su seguridad, protocolos, accesos y demás funcionalidades que permiten simular redes reales.

Palabras claves: CCNA, protocolos, enrutadores, conmutadores, seguridad.

ABSTRACT

This skills test is defined as learning based on the evaluative activities that were given in the Deepening Diploma CCNA, which allowed training based on concepts, connectivity, ethernet protocols in telecommunications, integrated networks LAN / WAN and the different configurations established for the devices incorporated in it; finding different learning exercises that allow the solution of various problems through educational resources presented by the university and by the different modules established in Cisco.

According to the above, It is necessary to address the different series of topics in order to acquire the necessary knowledge regarding the functionalities of routers and switches, which allows you to create small networks and apply the different components in terms of security, protocols accesses and other functionalities that allow simulating real networks.

Keywords: CCNA, protocols, routers, switches, security.

INTRODUCCIÓN

La presente “Prueba de habilidades prácticas” que se relaciona en base a los distintos entornos de aprendizaje del Diplomado de Profundización CISCO (Diseño e implementación de soluciones integradas LAN / WAN), permite desarrollar poco a poco los diferentes escenarios propuestos, incorporándose en las áreas de las telecomunicaciones, estableciendo redes de diferentes magnitudes, crear una documentación explicita en cada uno de los procesos, y demás, que establecen las tecnologías en Información; llegando a adquirir las habilidades necesarias en cada uno de los escenarios propuestos para aplicar el aprendizaje y las competencias establecidas en los diferentes módulos en donde a través de su comprensión se lleguen a solucionar los problemas en simulación y laboratorios de accesos remotos.

En el primer escenario propuesto se aplicará la configuración necesaria sobre una topología conformada por dispositivos de red el cual van a permitir plantear un esquema de direccionamiento IPv4 para las dos LAN que además se pueda administrar y realizar los ajustes necesarios en cada uno de ellos para que permita la comunicación entre sí, teniendo la disponibilidad de que las dos redes enlacen de una manera satisfactoria para poder simular una conectividad exitosa a la hora de emprender e implementar las diferentes topologías en la vida profesional.

En el segundo escenario se puede ver la realización de una topología más compleja, implementando el enrutamiento entre VLAN, realizando una configuración básica en el router para que permita la conectividad de las terminales a través de DHCP, creación de puertos Etherchannel en capa dos el cual permita usar el protocolo LACP para la negociación de envío de paquetes, la configuración de port-security en los puertos de accesos el cual se debe de permitir solamente cuatro terminales de conectividad a dicha red de conexión.

1. DESARROLLO ESCENARIO 1, PRUEBA DE HABILIDADES

Figura 1. Topología.

Fuente: Autor

En este primer escenario se configurarán los dispositivos de una red pequeña. Se debe de implementar y configurar un router, un switch; el cual se deben de administrar de forma segura, implementar equipos (sesenta hosts para la LAN uno y veinte hosts para la LAN dos), diseñar el esquema de direccionamiento IPv4 para las LAN propuestas la dirección suministrada realizará el subnetting.

1.1 PARTE 1: CONSTRUCCIÓN DE LA RED

Para poder construir la red se debe de abrir el programa de Cisco Packet Tracer con versión 8.2.0., al momento de abrir el programa solicitara ingresar las credenciales como correo y contraseña registrada con anterioridad en la página de Cisco. Luego, en el menú de barras seleccionamos opciones, y hay darle en perfil de usuario. Se ingresa los datos solicitados. Esto permitirá que queden registrados todas las actividades realizadas en el programa a nombre propio.

Luego de llenar los datos se procede a crear la red adecuada para el escenario. Se toma de la barra inferior izquierda los elementos necesarios tales como el Switch, Router, cables de conexiones y los 2 hosts, los cuales van a representar cada uno la cantidad de host en cada red LAN. Se realiza las conexiones adecuadas para los diferentes dispositivos; empezando a incorporar de primero el Switch, luego el Router, se le asigna los nombres a cada red, y la incorporación los hosts requeridos.

Luego se realiza la conexión por cableado a los equipos, se utiliza el “Copper Straight – Through”, verificando que estén conectados sobre los mismos puertos que pide la topología y así se tendrá listo los pasos requeridos en la parte 1.

1.2 PARTE 2: DESARROLLO DEL ESQUEMA DE DIRECCIONAMIENTO IP

Cada estudiante tomará el direccionamiento 172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.

Para realizar el llenado de la tabla de direccionamiento lo primero que se realiza es la verificación del cálculo, el cual se implementa en las dos subredes de direccionamiento. Si analizamos la ip (172.12.3.0) se clasifica de clase B, y que la máscara de red seria la 255.255.255.0, en donde se establece que la nueva dirección de red seria la 172.12.3.0/24 y que la dirección de broadcast seria la 172.12.3.255. Se toma la subred más grande que contiene 60 hosts, se toma la dirección ip 172.12.3.0, en donde esa subred puede tener la IP de red 172.12.3.0, con una máscara 255.255.255.0 (/24) en donde la primera IP a utilizar en el primer host seria 172.12.3.1 y que su última ip a utilizar en el host seria la 172.12.3.62, con la IP del broadcast 172.12.3.63 que siempre será la última dirección de la subred.

En el caso de la segunda subred que contiene 20 hosts, se analiza que desde la dirección IP 172.12.3.0 esa subred puede tener la IP de red 172.12.3.64, en donde su primera IP a utilizar en el primer host seria la 172.12.3.65 y que su última ip a utilizar en el host seria la 172.12.3.94, con la IP del broadcast 172.12.3.65.

Teniendo en cuenta el cálculo en base a la IP asignada se procede al llenado de la tabla de direccionamiento que se encuentra a continuación:

Tabla 1. Tabla de direccionamiento.

Item	Requerimiento
Dirección de Red	172.12.3.0
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.12.3.62
R1 G0/0/0	172.12.3.94
S1 SVI	172.12.3.2
PC-A	172.12.3.10
PC-B	172.12.3.74

Fuente: Autor

1.3 PARTE 3: CONFIGURACIÓN DE LOS ASPECTOS BÁSICOS

1.3.1 Paso 1: Configuración de los ajustes básicos. La configuración para el router uno se representa en la siguiente tabla en cuanto a las tareas, comandos y sus especificaciones de cada uno, a continuación:

Tabla 2. Configuración R1.

Tarea	Especificación
Desactivar la búsqueda DNS	DNS se desactiva para poder evitar pérdida de tiempo en alguna búsqueda de algún comando. EL comando de la tarea seria: Router>enable (este comando nos permite entrar al modo privilegiado) Router# configure terminal (este comando nos permite entrar en modo global especializados) Router(config)#no ip domain-lookup (Este es el comando que nos va a permitir desactivar la búsqueda DNS).
Nombre del router	R1 Router>enable (entramos al modo privilegiado) Router# configure terminal (entramos en modo global especializados) Router(config)#hostname R1 (comando que nos permite cambiar el nombre del equipo).
Nombre de dominio	ccna-sa.com R1>enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#ip domain-name ccna-sa.com (comando nos permite colocar el nombre del dominio de empresa o escuela, dependiendo en donde nos encontremos trabajando)
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass R1>enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#enable secret ciscoenpass (comando nos permite agregar la contraseña, pero cifrado)

Contraseña de acceso a la consola	ciscoconpass
	
	R1>enable (entramos al modo privilegiado)
	Password: (ingresamos la contraseña cifrada para el modo EXEC privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro R1)
	R1(config-line)#password ciscoconpass (se ingresa la contraseña)
	R1(config-line)#login (se activa la contraseña para que la pida al ingresar al sistema del R1)

Establecer la longitud mínima para las contraseñas	10 caracteres R1>enable (entramos al modo privilegiado) Password: (se ingresa la contraseña para el modo EXEC privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#security password min-length 10 (comando para establecer la longitud mínima de las contraseñas)

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin**
	Contraseña: **admin1pass**
	
	R1>enable (entramos al modo privilegiado)
	Password: (se ingresa la contraseña para el modo EXEC privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	“Como se va a crear un usuario administrativo debemos tener en cuenta que su nivel debe de ser 15”
	R1(config)#username admin privilege 15 secret admin1pass (este comando nos permite crear el usuario administrativo nivel 15 y asignarle la contraseña de modo secret)
	R1(config)#do write (este comando nos permite guardar el usuario creado)
	(Nota: solo está pidiendo la contraseña de acceso a la consola, se configura para que pida de primero el usuario. Se procede a configurar)
	R1>enable (entramos al modo privilegiado)
	Password: (se ingresa la contraseña para el modo EXEC privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro R1)

	R1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación)

Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1#enable (entramos al modo privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	R1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1#enable (entramos al modo privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	R1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)

Cifrar las contraseñas de texto no Cifrado	R1#enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#service password-encryption (comando el cual nos permite cifrar todas las contraseñas)
Configurar un banner MOTD	R1#configure terminal (entramos en modo global especializados) Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd "R1, Gabriel Eduardo Verdugo Medina, Ing. de Sistemas" (Este comando nos permitirá incluir el mensaje inicial)

Configuración de interface G0/0/0	R1#configure terminal (entramos en modo global especializados)
	R1(config)#interface gigabitEthernet 0/0/0 (con este comando llamamos a la interfaz el cual deseamos configurar)
	R1(config-if)#ip address 172.12.3.94 255.255.255.224 (al ser llamada le asignamos una ip con su mascara)
	R1(config-if)#no shutdown (luego encendemos el puerto para que quede listo)

Configuración de interface G0/0/1	R1#configure terminal (entramos en modo global especializados)
	R1(config)#interface gigabitEthernet 0/0/1 (con este comando llamamos a la interfaz el cual deseamos configurar)
	R1(config-if)#ip address 172.12.3.62 255.255.255.192 (al ser llamada le asignamos una ip con su mascara)
	R1(config-if)#no shutdown (luego encendemos el puerto para que quede listo)

Generar una clave de cifrado RSA	R1#configure terminal (entramos en modo global especializados)

	R1(config)#crypto key generate rsa general-keys modulus 1024 (comando el cual nos va a permitir generar una clave de cifrado RSA módulo de 1024 bits)

Fuente: Autor

La configuración del switch uno se representa a continuación en la siguiente tabla:

Tabla 3. Configuración SW1.

Tarea	**Especificación**
Desactivar la búsqueda DNS	Switch>enable (este comando nos permite entrar al modo privilegiado) Switch# configure terminal (este comando nos permite entrar en modo global especializados) Switch(config)#no ip domain-lookup (Este es el comando que nos va a permitir desactivar la búsqueda DNS)
Nombre del switch	Switch>enable (entramos al modo privilegiado) Switch# configure terminal (entramos en modo global especializados) Switch(config)#hostname S1 (comando que nos permite cambiar el nombre del equipo)
Nombre de dominio	S1#enable (entramos al modo privilegiado) S1#configure terminal (entramos en modo global especializados) S1(config)#ip domain-name ccna-sa.com (comando nos permite colocar el nombre del dominio de empresa o escuela, dependiendo en donde nos encontremos trabajando)
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass S1>enable (entramos al modo privilegiado) S1#configure terminal (entramos en modo global especializados) S1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola	ciscoconpass
	
	S1#conf term(entramos en modo global especializados)
	S1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro S1)
	S1(config-line)#password ciscoconpass (se ingresa la contraseña)
	S1(config-line)#login (se activa la contraseña para que la pida al ingresar al sistema del S1)

Apagar todos los puertos sin usar	F0/1-4, F0/7-24, G0/1-2
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#interface range fastEthernet 0/1-4 (anunciamos las interfaces que necesitamos apagar)
	S1(config-if-range)#shutdown (comando para apagar interfaces llamadas)
	S1(config-if-range)#interface range fastEthernet 0/7-24
	S1(config-if-range)#shutdown
	S1(config)#interface range gigabitEthernet 0/1-2
	S1(config-if-range)#shutdown

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin**
	Contraseña: **admin1pass**
	
	S1#configure terminal (entramos en modo global especializados)
	“Como se va a crear un usuario administrativo debemos tener en cuenta que su nivel debe de ser 15”
	S1(config)#username admin privilege 15 secret admin1pass (este comando nos permite crear el usuario administrativo nivel 15 y asignarle la contraseña de modo secret)
	S1(config)#do write (este comando nos permite guardar el usuario creado)
	(pero solo está pidiendo la contraseña de acceso a la consola, debería de pedir de primero el usuario. Se procede a configurar)
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro S1)
	S1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación)

Configure el inicio de sesión en las líneas VTY para que use la base de datos local	User Access Verification
	
	S1#conf term (entramos en modo global especializados)
	S1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	S1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)

Configurar las líneas VTY para que	S1#conf term (entramos en modo global especializados) S1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)

acepten únicamente las conexiones SSH	S1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)
Cifrar las contraseñas de texto no Cifrado	S1#conf term (entramos en modo global especializados) S1(config)#service password-encryption (comando el cual nos permite cifrar todas las contraseñas)
Configurar un banner MOTD	S1#conf term (entramos en modo global especializados) S1(config)#banner motd "S1, Gabriel Eduardo Verdugo Medina, Ing. de Sistemas" (Este comando nos permitirá incluir el mensaje inicial)
Generar una clave de cifrado RSA	S1#conf term (entramos en modo global especializados) S1(config)#crypto key generate rsa general-keys modulus 1024 (comando el cual nos va a permitir generar una clave de cifrado RSA módulo de 1024 bits)

Configure la interfaz de administración (SVI) en VLAN1	S1#conf term (entramos en modo global especializados)
	S1(config)#interface vlan 1 (luego llamamos la inter. vlan)
	S1(config-if)#ip address 172.12.3.2 255.255.255.0 (le asignamos la ip con su mascara)
	S1(config-if)#no shutdown (encendemos el puerto)

Fuente: Autor

1.3.2 Paso 2. Configuración de los equipos terminales. Se procede a configurar los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registrando las configuraciones de red de cada host en la tabla a continuación:

Tabla 4. Configuración PC-A.

Configuración de red de PC-A	
Descripción	FastEthernet 0
Dirección física	000D.BDB1.38E6
Dirección IPv4	172.12.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.12.3.62

Fuente: Autor

Tabla 5. Configuración PC-B.

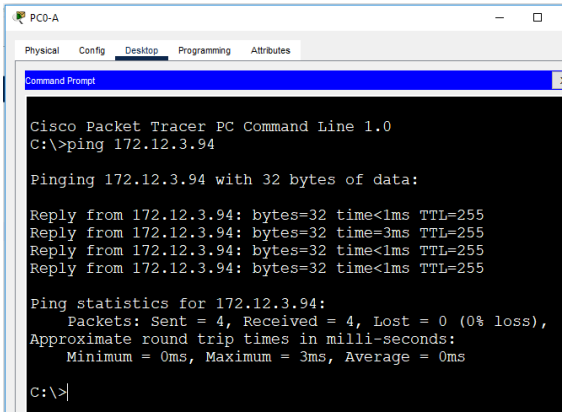
Configuración de red de PC-B	
Descripción	FastEthernet 0
Dirección física	000A.41CA.C153
Dirección IPv4	172.12.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.12.3.94

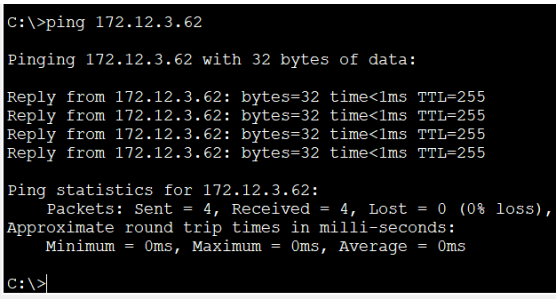
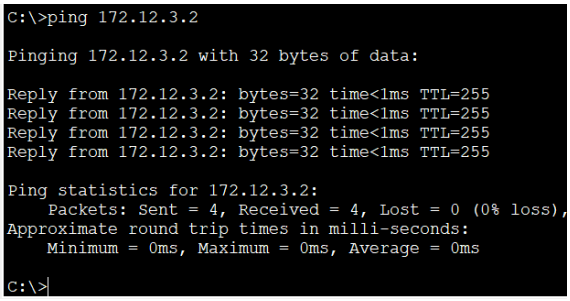
Fuente: Autor

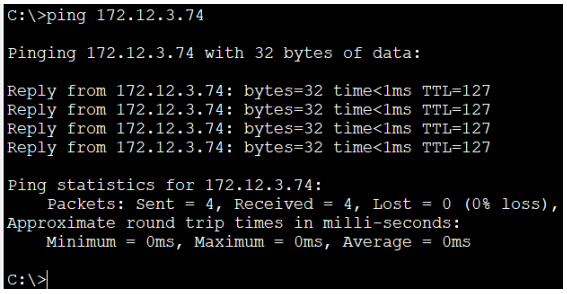
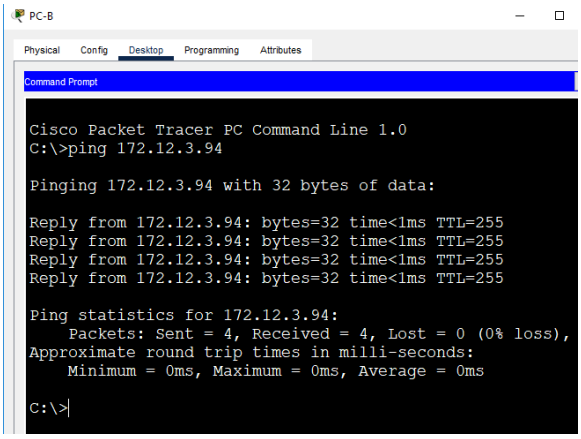
1.4 PARTE 4: VERIFICACIÓN DE LA CONECTIVIDAD, EXTREMO A EXTREMO

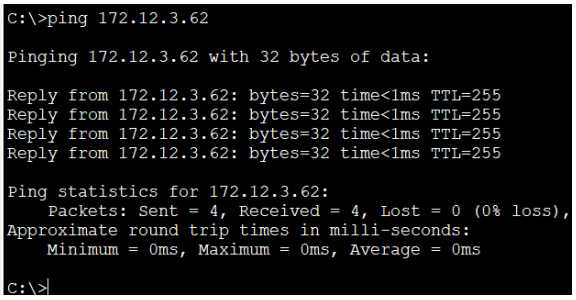
Utilice el comando ping para probar y verificar la conectividad entre todos los dispositivos de red, y proceda con el llenado de la tabla, tomando medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 6. Conectividad entre dispositivos.

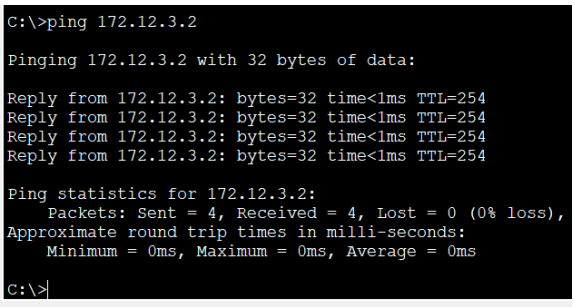
Desde	A	Dirección IP	Resultados
PC-A	R1 G0/0/0	172.12.3.94	Figura 2. Ping PC-A - R1 G0/0/0.  Fuente: Autor

			En la figura dos se logra evidenciar que el ping es exitoso, ya que la configuración de la red fue exitosa.
	R1 G0/0/1	172.12.3.62	Figura 3. Ping PC-A - R1 G0/0/1.  Fuente: Autor En la figura tres el ping es exitoso hacia la interfaz giga 0/0/1 ya que se logró la conectividad exitosamente.
	S1 VLAN 1	172.12.3.2	Figura 4. Ping PC-A - S1 VLAN 1.  Fuente: Autor En la figura cuatro se puede ver satisfactoriamente el ping realizado hacia la IP 172.12.3.2 ya que presenta la configuración correcta en base a la tabla de direccionamiento creada.

	PC-B	172.12.3.74	Figura 5. Ping PC-A – PC-B.  Fuente: Autor En la figura cinco también se logra con satisfacción de ping hacia la otra terminal ya que se encuentra con los parámetros satisfactorios de conectividad.
PC-B	R1 G0/0/0	172.12.3.94	Figura 6. Ping PC-B – R1 G0/0/0.  Fuente: Autor En la figura seis se evidencia la conectividad exitosa entre el PC-B hacia la IP 172.12.3.94 ya que su configuración se encuentra en la misma red.

<table>
<tr><td rowspan="2"></td><td>R1 G0/0/1</td><td>172.12.3.62</td><td>Figura 7. Ping PC-B – R1 G0/0/1.
 

Fuente: Autor

En la figura siete se evidencia pin exitoso hacia una interfaz específica del router, demostrando conectividad exitosa entre los componentes intermedios.</td></tr>
<tr><td>S1 VLAN1</td><td>172.12.3.2</td><td>Figura 8. Ping PC-B – S1 VLAN1.
 

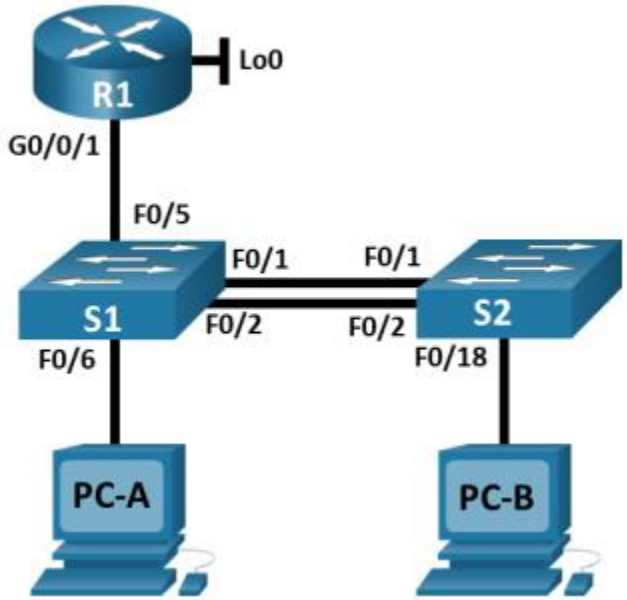
Fuente: Autor

En la figura ocho se logra evidenciar satisfactoriamente el enlace de conectividad entre el PC-B y la VLAN uno del Switch uno, ya que los elementos utilizados y su conectividad se encuentran configurados de manera satisfactoria en la red.</td></tr>
</table>

Fuente: Autor

2. DESARROLLO ESCENARIO 2, PRUEBA DE HABILIDADES

Figura 9. Topología.



Fuente: Autor

En el presente escenario se evidenciará la configuración de los dispositivos de una red pequeña. Se debe de 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. Se procederá a configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security para lograr los objetivos del segundo escenario.

A continuación, se referenciará las VLAN con sus respectivas identificaciones de cada una:

Tabla 7. Tabla de VLAN.

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

Fuente: Autor

2.1 TABLA DE ASIGNACIÓN DE DIRECCIONES

En nuestro caso se estaría usando el numero (12) para remplazar los direccionamientos establecidos en el presente escenario.

Tabla 8. Asignación de direcciones.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.12.8.1 /26	No corresponde
	2001:db8:acad:a::1 /64	No corresponde
R1 G0/0/1.30	10.12.8.65 /27	No corresponde
	2001:db8:acad:b::1 /64	No corresponde
R1 G0/0/1.40	10.12.8.97 /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	10.12.8.98 /29	10.12.8.97
	2001:db8:acad:c::98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.12.8.99 /29	10.12.8.97
	2001:db8:acad:c::99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminado IPv4
	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminado IPv4
	2001:db8:acad:b::50 /64	fe80::1

Fuente: Autor

2.2 PARTE 1: INICIALIZAR, RECARGAR Y CONFIGURAR LOS ASPECTOS BASICOS DE LOS DISPOSITIVOS

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

- Se procede a borrar las configuraciones de inicio, las VLAN del router y del switch, posteriormente se vuelve a cargar los dispositivos para verificar la configuración:

  Router>enable (entramos al modo privilegiado)
  Router#erase startup-config (comando que permite eliminar la configuración de inicio)
  [confirm] (se confirma para poder proceder)
  Router#reload (este comando permitirá reiniciar el dispositivo)
  [confirm] (se confirma y estará listo)
  Nota: Con estos mismos comandos se procede a borrar las configuraciones de inicio en el Sw.

  Luego se procede a borrar las VLAN en los Sw:
  Switch#delete flash:vlan.dat (Se entra al modo privilegiado y le damos al comando eliminar y se agrega comando donde se almacenan por lo general las vlan)
  [confirm] (se confirma y si tenemos vlan se eliminarán)

- Después de recargar el switch, se configura la plantilla SDM para que admita IPv6 según sea necesario y se procede a cargar el switch.
  Switch>enable (entramos al modo privilegiado)
  Switch#configure terminal (entramos en modo global especializados)
  Switch(config)#sdm prefer dual-ipv4-and-ipv6 default (este comando nos permitirá asignar en la plantilla SDM como preferencia dual (ipv4 y ipv6) para que se pueda trabajar sin problemas)
  Switch#reload (se vuelve a recargar el Sw)

  Luego que inicie verificamos:
  Switch(config)#sdm prefer ? (con este comando se verifica si aparecen las preferencias el dual ipv).

2.2.2 Paso 2: Configurar el router 1. Las tareas de configuración para el router uno se refleja a continuación en la siguiente tabla:

Tabla 9. Configuración R1.

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable (entramos al modo privilegiado) Router# configure terminal (entramos en modo global especializados) Router(config)#no ip domain-lookup (Este es el comando que nos va a permitir desactivar la búsqueda DNS)
Nombre del router	R1 Router>enable (entramos al modo privilegiado) Router# configure terminal (entramos en modo global especializados) Router(config)#hostname R1 (comando que nos permite cambiar el nombre del equipo)
Nombre de dominio	ccna-sa.com R1>enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#ip domain-name ccna-sa.com (comando nos permite colocar el nombre del dominio de empresa o escuela, dependiendo en donde nos encontremos trabajando)
Contraseña cifrada para el modo EXEC Privilegiado	class R1>enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#enable secret class. (comando nos permite agregar la contraseña, pero cifrado)

Contraseña de acceso a la consola	Cisco
	
	R1>enable (entramos al modo privilegiado)
	Password: (ingresamos la contraseña cifrada para el modo EXEC privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro R1)
	R1(config-line)#password cisco (se ingresa la contraseña)
	R1(config-line)#login (se activa la contraseña para que la pida al ingresar al sistema del R1)

Establecer la longitud mínima para las Contraseñas	5 caracteres Password: (se ingresa la contraseña de acceso a la consola) R1>enable (entramos al modo privilegiado)

	Password: (se ingresa la contraseña para el modo EXEC privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#security password min-length 5 (comando para establecer la longitud mínima de las contraseñas)

Crear un usuario administrativo en la
base de datos local
	Nombre de usuario: **admin**
	Password: **admin1pass**
	
	R1>enable (entramos al modo privilegiado)
	Password: (se ingresa la contraseña para el modo EXEC privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	“Como se va a crear un usuario administrativo debemos tener en cuenta que su nivel debe de ser 15”
	R1(config)#username admin privilege 15 secret admin1pass (este comando nos permite crear el usuario administrativo nivel 15 y asignarle la contraseña de modo secret)
	R1(config)#do write (este comando nos permite guardar el usuario creado)
	(Solo está pidiendo la contraseña de acceso a la consola, debería de pedir de primero el usuario. Se procede a configurar)
	R1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro R1)
	R1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación)

Configurar el inicio de sesión en las
líneas VTY para que use la base de datos local
	R1#enable (entramos al modo privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	R1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)

Configurar VTY solo aceptando SSH	R1#enable (entramos al modo privilegiado)
	R1#configure terminal (entramos en modo global especializados)
	R1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	R1(config-line)#transport input ssh (este comando nos permite configurar VTY para que solo acepte SSH)

Cifrar las contraseñas de texto no cifrado	R1#enable (entramos al modo privilegiado) R1#configure terminal (entramos en modo global especializados) R1(config)#service password-encryption (comando el cual nos permite cifrar todas las contraseñas)

Configure un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. R1#configure terminal (entramos en modo global especializados) R1(config)#banner motd "R1, Gabriel Eduardo Verdugo Medina, Ing. de Sistemas" (Este comando nos permitirá incluir el mensaje inicial)
Habilitar el routing IPv6	R1#configure terminal (entramos en modo global especializados) R1(config)#ipv6 unicast-routing (Este comando permite habilitar el routing IPv6)

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 terminal (entramos en modo global especializados)
	R1(config)#interface gigabitEthernet 0/0/1.20 (Entramos a la interfaz el cual deseamos configurar, en este caso es la interfaz con su subinterfaz)
	R1(config-subif)#encapsulation dot1Q 20 (se activa este protocolo para que el router tenga enlace troncal de la VLAN)
	R1(config-subif)#ip address 10.12.8.1 255.255.255.192 (se le asigna la ipv4)
	R1(config-subif)#ipv6 address fe80::1 link-local (se le establece la dirección local de enlace IPv6)
	R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 (se le asigna la ipv6)
	
	“Posteriormente, se realiza el mismo procedimiento con las siguientes subinterfaces que tenemos en la tabla”
	
	R1(config)#interface gigabitEthernet 0/0/1.30
	R1(config-subif)#encapsulation dot1Q 30
	R1(config-subif)#ip address 10.12.8.65 255.255.255.224
	R1(config-subif)#ipv6 address fe80::1 link-local
	R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
	R1(config-subif)#interface gigabitEthernet 0/0/1.40
	R1(config-subif)#encapsulation dot1Q 40
	R1(config-subif)#ip address 10.12.8.97 255.255.255.248
	R1(config-subif)#ipv6 address fe80::1 link-local
	R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
	R1(config-subif)#exit
	R1(config)#interface gigabitEthernet 0/0/1 (luego llamamos la interfaz real)

	R1(config-if)#no shutdown (y la encendemos para que funcione nuestras subinterfaces)

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#configure terminal (entramos en modo global especializados)
	R1(config)#interface loopback 0 (con este comando se crea el loopback cero, se activa inmediatamente)
	R1(config-if)#ip address 209.165.201.1 255.255.255.224 (se agrega la ipv4 a la loopback)
	R1(config-if)#ipv6 address 2001:db8:acad:209::1/64(se agrega la ipv6 a la loopback)
	R1(config-if)#ipv6 address fe80::1 link-local (se agrega la dirección local de enlace IPv6 a la loopback)
	R1(config-if)#exit (nos salimos para que quede todo guardado)

Generar una clave de cifrado RSA	Módulo de 1024 bits R1#configure terminal (entramos en modo global especializados) R1(config)#crypto key generate rsa general-keys modulus 1024 (comando el cual nos va a permitir generar una clave de cifrado RSA módulo de 1024 bits)

Fuente: Autor

2.2.3 Paso 3: Configuración del switch 1 y 2. Las tareas establecidas para la configuración de los switches se reflejarán a continuación en la siguiente tabla:

Tabla 10. Configuración Switch 1 Y 2.

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable (entramos al modo privilegiado) Switch# configure terminal (entramos en modo global especializados) Switch(config)#no ip domain-lookup (Este es el comando que nos va a permitir desactivar la búsqueda DNS)
Nombre del switch	S1 o S2, según proceda Switch>enable (entramos al modo privilegiado)

	Switch# configure terminal (entramos en modo global especializados) Switch(config)#hostname S1 (comando que nos permite cambiar el nombre del equipo)
Nombre de dominio	ccna-sa.com S1#enable (entramos al modo privilegiado) S1#configure terminal (entramos en modo global especializados) S1(config)#ip domain-name ccna-sa.com (comando nos permite colocar el nombre del dominio de empresa o escuela, dependiendo en donde nos encontremos trabajando)
Contraseña cifrada para el modo EXEC Privilegiado	class S1>enable (entramos al modo privilegiado) S1#configure terminal (entramos en modo global especializados) S1(config)#enable secret class (comando nos permite colocar la contraseña de EXEC Privilegiado cifrado)

Contraseña de acceso a la consola	cisco
	
	S1>enable (entramos al modo privilegiado)
	Password: (ingresamos la contraseña cifrada para el modo EXEC privilegiado)
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro S1)
	S1(config-line)#password cisco (se ingresa la contraseña)
	S1(config-line)#login (se activa la contraseña para que la pida al ingresar al sistema del S1)

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Password: (se ingresa la contraseña de acceso a la consola) S1>enable (entramos al modo privilegiado) Password: (se ingresa la contraseña para el modo EXEC privilegiado) S1#configure terminal (entramos en modo global especializados) “Como se va a crear un usuario administrativo debemos tener en cuenta que su nivel debe de ser 15” S1(config)#username admin privilege 15 secret admin1pass (este comando nos permite crear el usuario administrativo nivel 15 y asignarle la contraseña de modo secret)

	S1(config)#do write (este comando nos permite guardar el usuario creado)
	“Solo está pidiendo la contraseña de acceso a la consola, debería de pedir de primero el usuario. Se procede a configurar”
	S1(config)#line console 0 (comando para colocarle la contraseña a la consola, siendo la 0(cero) ya que es la única entrada de consola que tiene nuestro S1)
	S1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación)
	“Ya nos debe de pedir el usuario de primero para poder ingresar al S1”

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#conf term (entramos en modo global especializados)
	S1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	S1(config-line)#login local (este comando nos permite la configuración de línea habilita la base de datos local para la autenticación, pero por nuestras sesiones Telnet)

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1#enable (entramos al modo privilegiado)
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#line vty 0 15 (este comando nos sirve para establecer sesiones Telnet, habilitar los servicios de SSH)
	S1(config-line)#transport input ssh (este comando nos permite configurar VTY para que solo acepte SSH)

Cifrar las contraseñas de texto no cifrado	S1#conf term (entramos en modo global especializados) S1(config)#service password-encryption (comando el cual nos permite cifrar todas las contraseñas)
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. S1#conf term (entramos en modo global especializados) S1(config)#banner motd "S1, Gabriel Eduardo Verdugo Medina, Ing. de Sistemas" (Este comando nos permitirá incluir el mensaje inicial)
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1#conf term (entramos en modo global especializados) S1(config)#crypto key generate rsa general-keys modulus 1024 (comando el cual nos va a permitir generar una clave de cifrado RSA módulo de 1024 bits)
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2**

	Establecer la dirección IPv6 de capa 3
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#interface VLAN 40 (luego llamamos la inter. VLAN asignada)
	S1(config-if)#ip address 10.12.8.98 255.255.255.248 (le asignamos la ip con su mascara)
	S1(config-if)#ipv6 address fe80::98 link-local (se le establece la dirección local de enlace IPv6)
	S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 (se le agrega la ipv6)
	S1(config-if)#no shutdown (y la encendemos para que funcione la inter. VLAN)
	S2(config)#interface vlan 40
	S2(config-if)#ip address 10.12.8.99 255.255.255.248
	S2(config-if)#ipv6 address fe80::99 link-local
	S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
	S2(config-if)#no shutdown

Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.12.8.97 para IPv4 S1#configure terminal (entramos en modo global especializados) S1(config)#ip default-gateway 10.12.8.97 (este comando nos permitirá asignar la ip de gateway)

Fuente: Autor

2.3 PARTE 2: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

2.3.1 Paso 1: Configuración del switch 1.

Tabla 11. Configuración Infraestructura Switch 1.

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes S1#configure terminal (entramos en modo global especializados) S1(config)#VLAN 20 (creamos nuestra VLAN)

	S1(config-vlan)#name Docentes (le asignamos un nombre a nuestra VLAN)

	VLAN 30, nombre Estudiantes
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#VLAN 30 (creamos nuestra VLAN)
	S1(config-vlan)#name Estudiantes (le asignamos un nombre a nuestra VLAN)

	VLAN 40, nombre Invitados
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#vlan 40 (creamos nuestra VLAN)
	S1(config-vlan)#name Invitados (le asignamos un nombre a nuestra VLAN)

	VLAN 50, nombre Usuarios
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#vlan 50 (creamos nuestra VLAN)
	S1(config-vlan)#name Usuarios (le asignamos un nombre a nuestra VLAN)

	VLAN 56, nombre Native
	
	S1#configure terminal (entramos en modo global especializados)
	S1(config)#vlan 56 (creamos nuestra VLAN)
	S1(config-vlan)#name Native (le asignamos un nombre a nuestra VLAN)

Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Interfaces F0/1, F0/2 y F0/5
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface fastEthernet 0/1(Ingresamos a la configuración de la interfaz)
	S1(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)
	S1(config-if)#switchport trunk native VLAN 56 (se especifica la vlan nativa)
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface fastEthernet 0/2(Ingresamos a la configuración de la interfaz)
	S1(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)

	S1(config-if)#switchport trunk native vlan 56 (se especifica la vlan nativa)
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface fastEthernet 0/5(Ingresamos a la configuración de la interfaz)
	S1(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)
	S1(config-if)#switchport trunk native vlan 56 (se especifica la vlan nativa)

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#conf t (Ingresamos a la configuración global)
	S1(config)#interface range fastEthernet 0/1-2 (anunciamos las interfaces que necesitamos)
	S1(config-if-range)#channel-group 1 mode active (este comando permite asignar el grupo channel, el modo el cual se va a trabajar “si es por protocolo PAgP seria por modo “desirable” o “automático”, y si es por protocolo LACP seria por modo “active” o “passive””)
	S1(config-if-range)#exit (salimos)
	S1(config)#interface port-channel 1(luego este comando nos permite llamar la interfaz del puerto channel con el grupo creado anteriormente)
	S1(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)

Configurar el puerto de acceso de host para VLAN 20	Interface F0/6
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface fastEthernet 0/6 (anunciamos la interfaz a trabajar)
	S1(config-if)#switchport mode Access (se configura la interfaz en modo de acceso)
	S1(config-if)#switchport access VLAN20 (se configura el puerto a la VLAN 20)

Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface fastEthernet 0/6 (anunciamos la interfaz a trabajar)
	S1(config-if)#switchport port-security maximum 4 (se configura la cantidad de MAC permitidas en el puerto)

Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar
	
	S1#configure terminal (Ingresamos a la configuración global)
	S1(config)#interface range fastEthernet 0/3-4 (llamamos al rango de las interfaces a configurar)
	S1(config-if-range)#switchport mode Access (se configura la interfaz en modo de acceso)
	S1(config-if-range)#switchport access VLAN 50 (se configuran los puertos a la VLAN 50)
	S1(config-if-range)#description Puertos apagados (se les agrega una descripción a puertos seleccionados)
	S1(config-if-range)#shutdown (se apagan puertos)
	
	S1#configure terminal
	S1(config)#interface range fastEthernet 0/7-24
	S1(config-if-range)#switchport mode Access
	S1(config-if-range)#switchport access VLAN 50
	S1(config-if-range)#description Puertos apagados
	S1(config-if-range)#shutdown
	
	S1#configure terminal
	S1(config)#interface range gigabitEthernet 0/1-2
	S1(config-if-range)#switchport mode Access
	S1(config-if-range)#switchport access VLAN 50
	S1(config-if-range)#description Puertos apagados
	S1(config-if-range)#shutdown

Fuente: Autor

2.3.2 Paso 2: Configure el switch 2. Entre las tareas de configuración del Switch dos se deben de incluir las siguientes tareas:

Tabla 12. Configuración Infraestructura del Switch 2.

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes S2#configure terminal (entramos en modo global especializados) S2(config)#VLAN 20 (creamos nuestra VLAN)

	S2(config-vlan)#name Docentes (le asignamos un nombre a nuestra VLAN)

	VLAN 30, nombre Estudiantes
	
	S2#configure terminal (entramos en modo global especializados)
	S2(config)# VLAN 30 (creamos nuestra VLAN)
	S2(config-vlan)#name Estudiantes (le asignamos un nombre a nuestra VLAN)

	VLAN 40, nombre Invitados
	
	S2#configure terminal (entramos en modo global especializados)
	S2(config)# VLAN 40 (creamos nuestra VLAN)
	S2(config-vlan)#name Invitados (le asignamos un nombre a nuestra VLAN)

	VLAN 50, nombre Usuarios
	
	S2#configure terminal (entramos en modo global especializados)
	S2(config)# VLAN 50 (creamos nuestra VLAN)
	S2(config-vlan)#name Usuarios (le asignamos un nombre a nuestra VLAN)

	VLAN 56, nombre Native
	
	S2#configure terminal (entramos en modo global especializados)
	S2(config)# VLAN 56 (creamos nuestra VLAN)
	S2(config-vlan)#name Native (le asignamos un nombre a nuestra VLAN)

Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Interfaces F0/1 y F0/2
	
	S2#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface fastEthernet 0/1(Ingresamos a la configuración de la interfaz)
	S2(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)
	S2(config-if)#switchport trunk native VLAN 56 (se especifica la vlan nativa)
	
	S2#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface fastEthernet 0/2(Ingresamos a la configuración de la interfaz)
	S2(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)

	S2(config-if)#switchport trunk native VLAN 56 (se especifica la vlan nativa)

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#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface range fastEthernet 0/1-2 (anunciamos las interfaces que necesitamos)
	S2(config-if-range)#channel-group 1 mode active (este comando permite asignar el grupo channel, el modo el cual se va a trabajar “si es por protocolo PAgP seria por modo “desirable” o “automático”, y si es por protocolo LACP seria por modo “active” o “passive””)
	S2(config-if-range)#exit (salimos)
	S2(config)#interface port-channel 1(luego este comando nos permite llamar la interfaz del puerto channel con el grupo creado anteriormente)
	S2(config-if)#switchport mode trunk (se configura la interfaz en enlace troncal)

Configurar el puerto de acceso de host para VLAN 30	Interfaz F0/18
	
	S2#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface fastEthernet 0/18 (anunciamos la interfaz a trabajar)
	S2(config-if)#switchport mode Access (se configura la interfaz en modo de acceso)
	S2(config-if)#switchport access VLAN 30 (se configura el puerto a la VLAN 30)

Configure port-security en los access ports	permite 4 MAC addresses
	
	S2#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface fastEthernet 0/18 (anunciamos la interfaz a trabajar)
	S2(config-if)#switchport port-security maximum 4 (se configura la cantidad de MAC permitidas en el puerto)

Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar.
	
	S2#configure terminal (Ingresamos a la configuración global)
	S2(config)#interface range fastEthernet 0/3-17 (llamamos al rango de las interfaces a configurar)
	S2(config-if-range)#switchport mode access (se configura la interfaz en modo de acceso)

	S2(config-if-range)#switchport access VLAN 50 (se configuran los puertos a la VLAN 50)
	S2(config-if-range)#description Puertos apagados (se les agrega una descripción a puertos seleccionados)
	S2(config-if-range)#shutdown (se apagan puertos)
	
	S2#configure terminal
	S2(config)#interface range fastEthernet 0/19-24
	S2(config-if-range)#switchport mode access
	S2(config-if-range)#switchport access VLAN 50
	S2(config-if-range)#description Puertos apagados
	S2(config-if-range)#shutdown
	
	S2#configure terminal
	S2(config)#interface range gigabitEthernet 0/1-2
	S2(config-if-range)#switchport mode access
	S2(config-if-range)#switchport access VLAN 50
	S2(config-if-range)#description Puertos apagados
	S2(config-if-range)#shutdown

Fuente: Autor

2.4 PARTE 3: CONFIGURAR EL SOPORTE DE HOST

2.4.1 Paso 1: Configurar el router 1. Las tareas de configuración para el router uno debe de incluir las siguientes tareas:

Tabla 13. Configuración host Router 1.

Tarea	Especificación

Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
	
	R1#configure terminal (Ingresamos a la configuración global)
	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 (se crea la ruta para ipv4 hacia la interfaz Loopback)
	R1(config)#ipv6 route ::/0 loopback 0 (se crea la ruta para ipv6 hacia la interfaz Loopback)

Configurar IPv4 DHCP para	Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio

VLAN 20	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#conf t (Ingresamos a la configuración global)
	R1(config)#ip dhcp pool DHCP-VLAN20 (comando para configurar dhcp en vlan 20)
	R1(dhcp-config)#domain-name unad-ccna-sa.net (comando para asignarle nombre a dominio)
	R1(dhcp-config)#network 10.12.8.0 255.255.255.192 (se le asigna la ip con su mascara)
	R1(dhcp-config)#default-router 10.12.8.1 (se le asigna la ip de la puerta en enlace)
	R1(dhcp-config)#exit
	R1(config)#ip dhcp excluded-address 10.12.8.1 10.12.8.52 (se excluyen las ip que no debe de tomar por dhcp)

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 router para la subred involucrada.
	
	R1#conf t (Ingresamos a la configuración global)
	R1(config)#ip dhcp pool DHCP-VLAN30 (comando para configurar dhcp en vlan 30)
	R1(dhcp-config)#domain-name unad-ccna-sb.net (comando para asignarle nombre a dominio)
	R1(dhcp-config)#network 10.12.8.64 255.255.255.224 (se le asigna la ip con su mascara)
	R1(dhcp-config)#default-router 10.12.8.65(se le asigna la ip de la puerta en enlace)
	R1(dhcp-config)#exit
	R1(config)#ip dhcp excluded-address 10.12.8.65 10.12.8.89(se excluyen las ip que no debe de tomar por dhcp)

Fuente: Autor

2.4.2 Paso 2: Configuración de los servidores. Se procede a configurar los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y se le asigna estáticamente las direcciones IPv6 GUA y link Local. Después de configurar cada servidor, se procede a registrar cada configuración de red de cada host en sus respectivas tablas a continuación:

Tabla 14. Configuración host PC-A.

Configuración de red de PC-A	
Descripción	unad-ccna-sa.net
Dirección física	0050.0F7D.2428
Dirección IP	10.12.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.12.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Tabla 15. Configuración host PC-B.

Configuración de red de PC-B	
Descripción	unad-ccna-sb.net
Dirección física	0001.4230.D936
Dirección IP	10.12.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.12.8.65
Gateway predeterminado IPv6	FE80::1

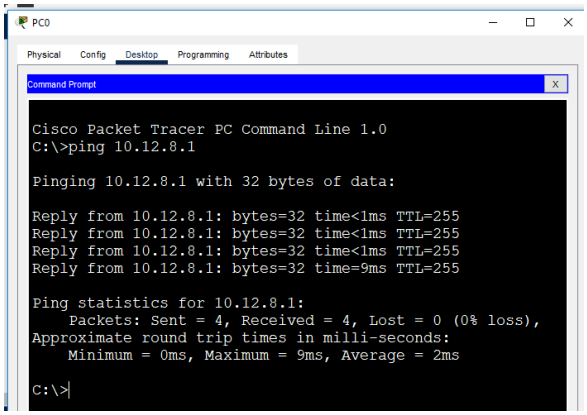
Fuente: Autor

2.5 PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

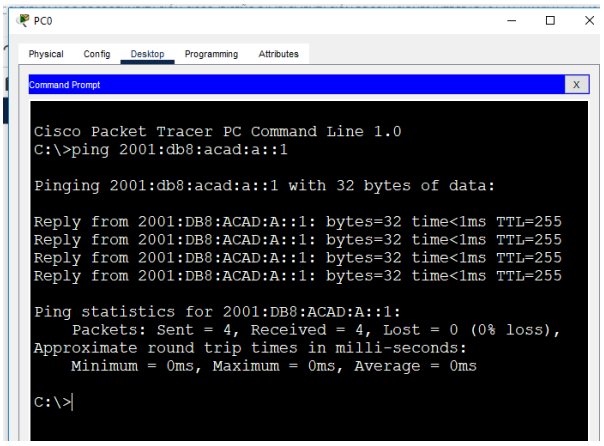
Se procede a utilizar el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos que se encuentran en la red.

Se realiza el llenado de la siguiente tabla para verificar metódicamente la conectividad con cada uno de los dispositivos de la red, teniendo en cuentan que si la conectividad en alguno falla se debe tomar medidas correctivas para lograr la conectividad satisfactoriamente:

Tabla 16. Verificación de Conectividad.

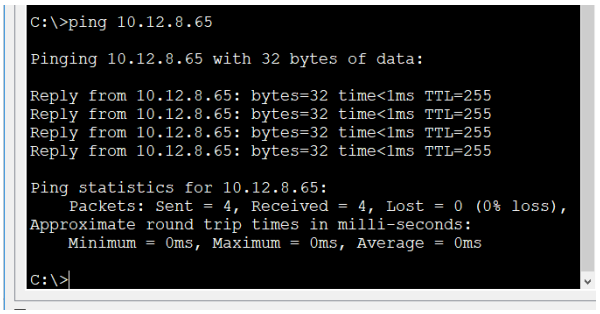
<table>
<tr><th>Desde</th><th>A</th><th></th><th>Dirección IP</th><th>Resultados de ping</th></tr>
<tr><td rowspan="2">PC-A</td><td rowspan="2">R1, G0/0/1.2</td><td>IPv4</td><td>10.12.8.1 /26</td><td>Figura 10. Ping PC-A a 10.12.8.1.
 

Fuente: Autor

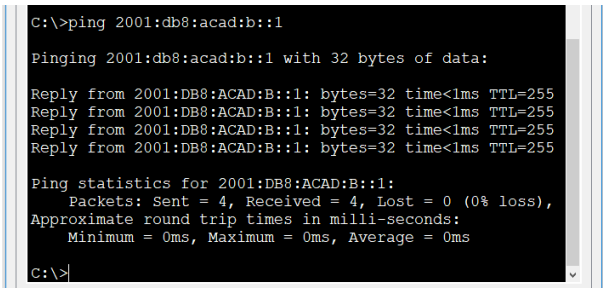
Se verifica la conectividad exitosa entre el pc-a y la ip establecida ya que su conectividad es acorde a lo solicitado en la guía.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:a::1</td><td>Figura 11. Ping PC-A a 2001:db8:acad:a::1.
 

Fuente: Autor

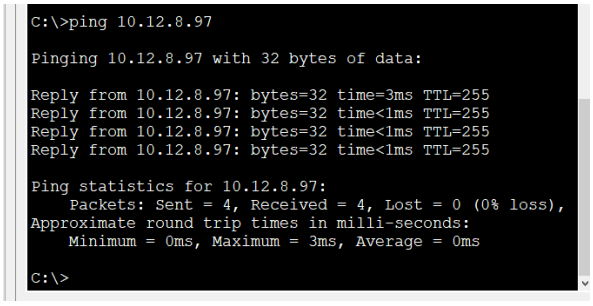
Se comprueba ping exitoso entre el pc-a y la ipv6 del R1, G0/0/1.2, ya que su configuración en la subinterfaz es exitosa.</td></tr>
</table>

<table>
<tr><td rowspan="3"></td><td rowspan="2">R1, G0/0/1.3</td><td>IPv4</td><td>10.12.8.65</td><td>Figura 12. Ping PC-A a 10.12.8.65
 

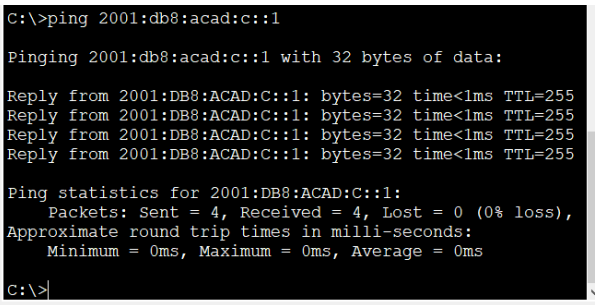
Fuente: Autor

Se evidencia ping exitoso entre el pc-a y la ip 10.12.8.65 ya que se encuentra exitoso de extremo a extremo.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b::1</td><td>Figura 13. Ping PC-A a 2001:db8:acad:b::1
 

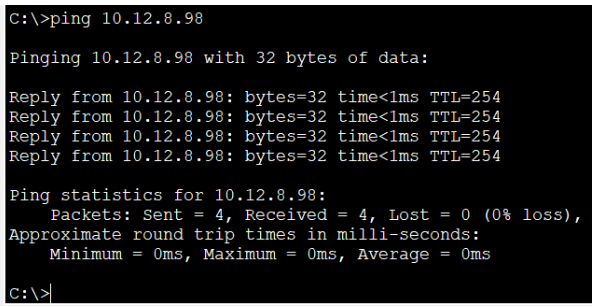
Fuente: Autor

Se encuentra satisfactorio ping desde el pc-a a la ipv6 2001:db8:acad:b::1 ya que su configuración es excelente.</td></tr>
<tr><td>R1, G0/0/1.4</td><td>IPv4</td><td>10.12.8.97</td><td>Figura 14. Ping PC-A a 10.12.8.97
 

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

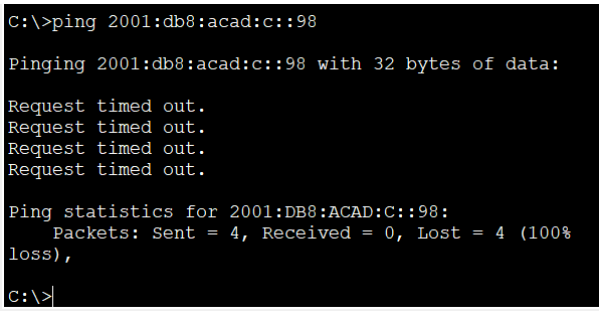
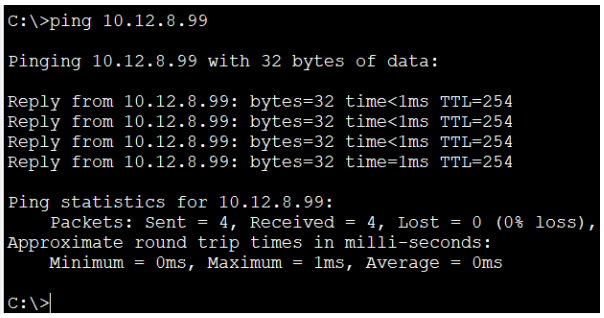
<table>
<tr><td rowspan="3"></td><td rowspan="2"></td><td></td><td></td><td>Se logra identificar ping exitoso en la figura 14, ya que se logró cumplir los pasos establecidos en el escenario.</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::1</td><td>Figura 15. Ping PC-A a 2001:db8:acad:c::1
 

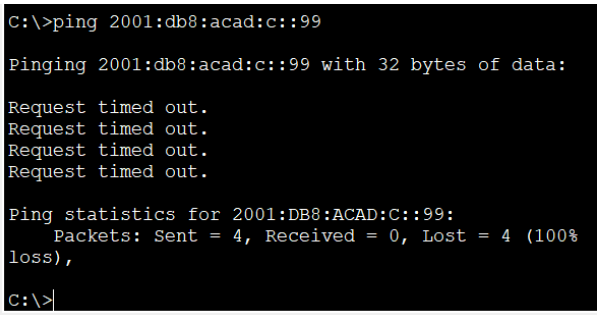
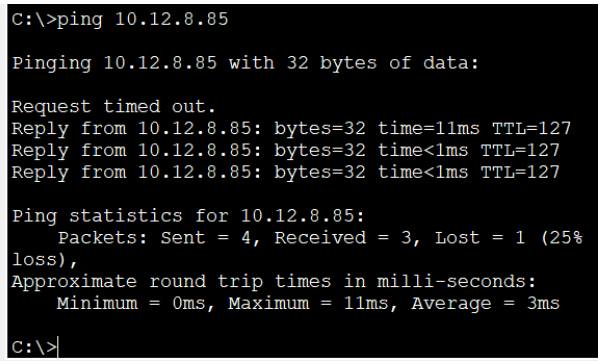
Fuente: Autor

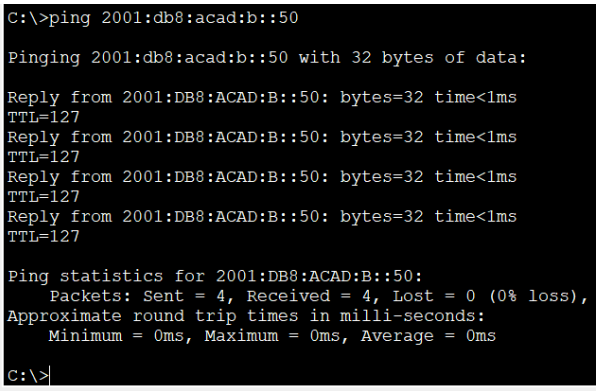
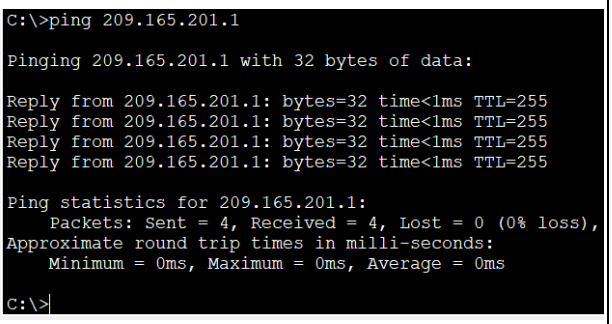
Se evidencia ping exitoso entre el pc-a y la ivp6 2001:db8:acad:c::1 ya que se configuró el router satisfactoriamente.</td></tr>
<tr><td>S1, VLAN 40</td><td>IPv4</td><td>10.12.8.98</td><td>Figura 16. Ping PC-A a 10.12.8.98
 

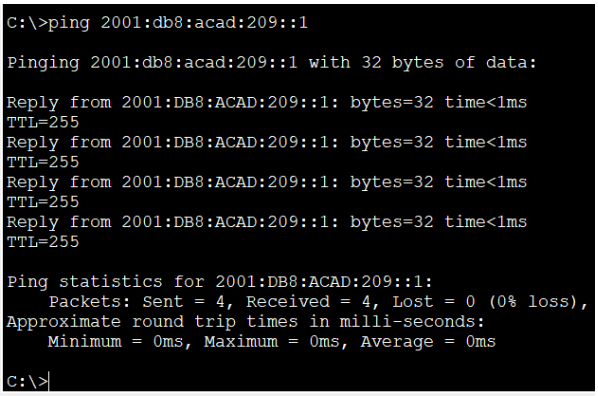
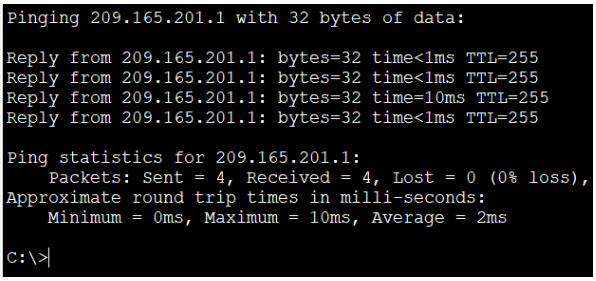
Fuente: Autor

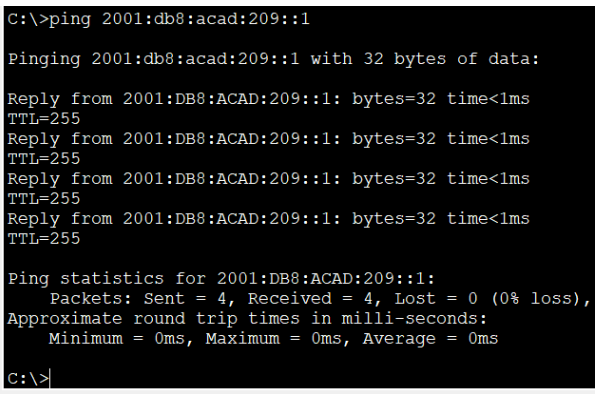
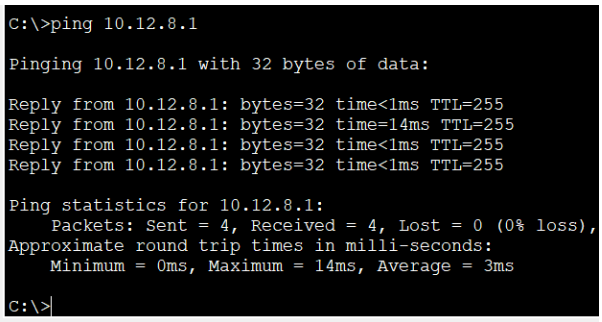
En la figura 16 se evidencia ping exitoso entre las ip establecidas ya que su configuración en la VLAN 40 estuvo correcta.</td></tr>
</table>

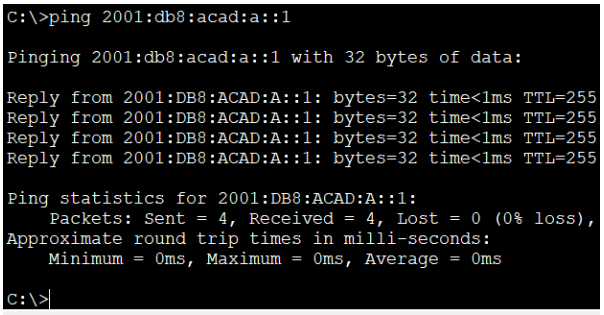
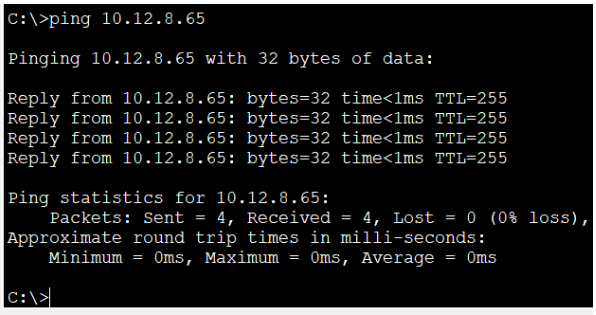
		IPv6	2001:db8:acad:c::98	Figura 17. Ping PC-A a 2001:db8:acad:c::98  Fuente: Autor El ping en este caso no es satisfactorio por un problema del IOS del switch, su configuración realizada en el escenario está correcta.
	S2, VLAN 40	IPv4	10.12.8.99	Figura 18. Ping PC-A a 10.12.8.99  Fuente: Autor Se establece ping exitoso entre el pc-a a la ip 10.12.8.99 ya que su conexión es válida para los requerimientos del escenario.

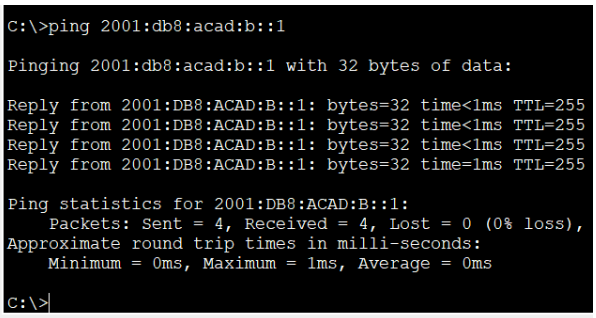
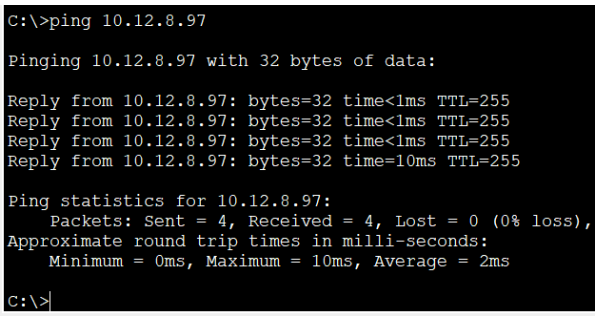
		IPv6	2001:db8:acad:c::99	Figura 19. Ping PC-A a 2001:db8:acad:c::99  Fuente: Autor El ping en este caso no es satisfactorio por un problema del IOS del switch, su configuración realizada en el escenario está correcta.
	PC-B	IPv4	10.12.8.85	Figura 20. Ping PC-A a 10.12.8.85  Fuente: Autor Se evidencia ping exitoso entre las ip establecidas ya que su estructura se encuentra bien estructurada.

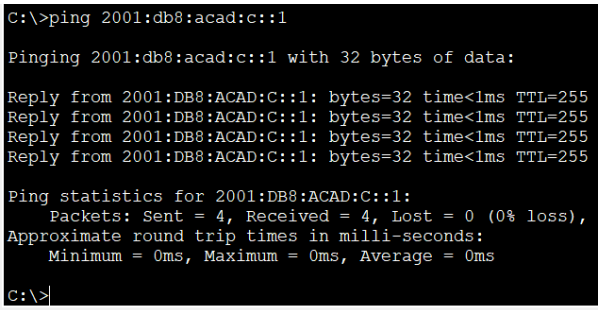
		IPv6	2001:db8:acad:b::50	Figura 21. Ping PC-A a 2001:db8:acad:b::50  Fuente: Autor En la figura 21 también se logra con satisfacción de ping hacia la otra terminal ya que se encuentra con los parámetros satisfactorios de conectividad.
	R1 Bucle 0	IPv4	209.165.201.1 /27	Figura 22. Ping PC-A a 209.165.201.1  Fuente: Autor Se evidencia ping exitoso entre el pc-a y la ip 209.165.201.1 ya que se configuró el router satisfactoriamente.

		IPv6	2001:db8:acad:209::1 /64	Figura 23. Ping PC-A a 2001:db8:acad:209::1  Fuente: Autor Se establece ping exitoso entre el pc-a a la ipv6 2001:db8:acad:209::1 ya que su conexión es válida para los requerimientos del escenario.
PC-B	R1 Bucle 0	IPv4	209.165.201.1 /27	Figura 24. Ping PC-B a 209.165.201.1  Fuente: Autor Se verifica la conectividad exitosa entre el pc-b y la ip establecida ya que su conectividad es acorde a lo solicitado en la guía.

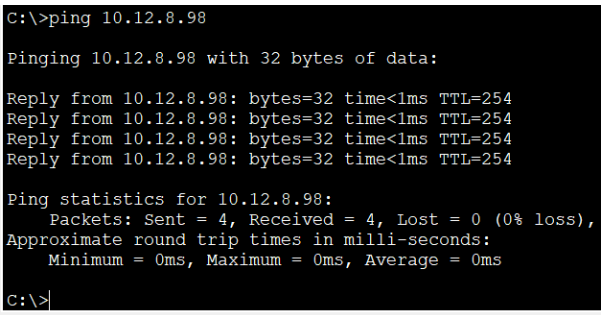
		IPv6	2001:db8:acad:209::1 /64	Figura 25. Ping PC-B a 2001:db8:acad:209::1  Fuente: Autor Se comprueba ping exitoso entre el pc-b y la ipv6 del R1 del bucle 0, ya que su configuración es exitosa.
	R1, G0/0/1.2	IPv4	10.12.8.1 /26	Figura 26. Ping PC-B a 10.12.8.1  Fuente: Autor Se evidencia ping exitoso entre el pc-b y la ip 10.12.8.1 ya que se encuentra exitoso de extremo a extremo.

		IPv6	2001:db8:acad:a::1	Figura 27. Ping PC-B a 2001:db8:acad:a::1  Fuente: Autor Se encuentra satisfactorio ping desde el pc-b a la ipv6 2001:db8:acad:a::1 ya que su configuración es excelente.
	R1, G0/0/1.3	IPv4	10.12.8.65	Figura 28. Ping PC-B a 10.12.8.65  Fuente: Autor Se logra identificar ping exitoso en la figura 28, ya que se logró cumplir los pasos establecidos en el escenario.

		IPv6	2001:db8:acad:b::1	Figura 29. Ping PC-B a 2001:db8:acad:b::1  Fuente: Autor Se evidencia ping exitoso entre el pc-b y la ivp6 2001:db8:acad:b::1 ya que se configuró el router satisfactoriamente.
	R1, G0/0/1.4	IPv4	10.12.8.97	Figura 30. Ping PC-B a 10.12.8.97  Fuente: Autor En la figura 30 se evidencia ping exitoso entre las ip establecidas ya que su configuración en el R1, G0/0/1.4 estuvo correcta.

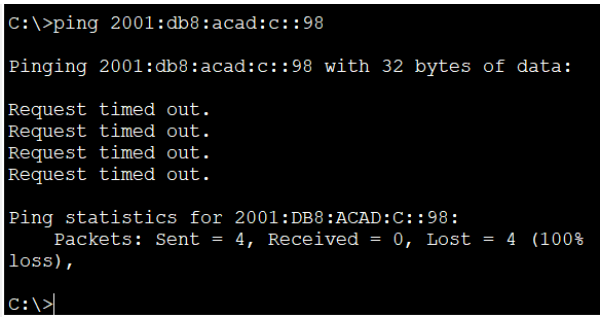
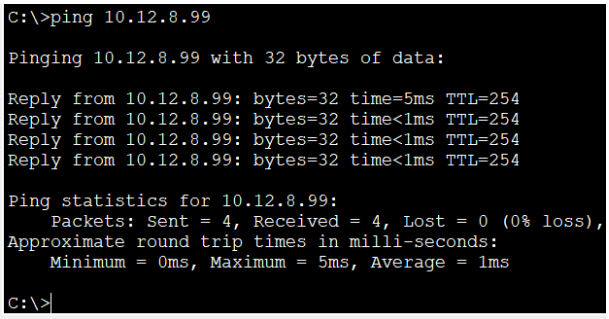
<table>
<tr><td rowspan="2"></td><td></td><td>IPv6</td><td>2001:db8:acad:c::1</td><td>Figura 31. Ping PC-B a 2001:db8:acad:c::1
 

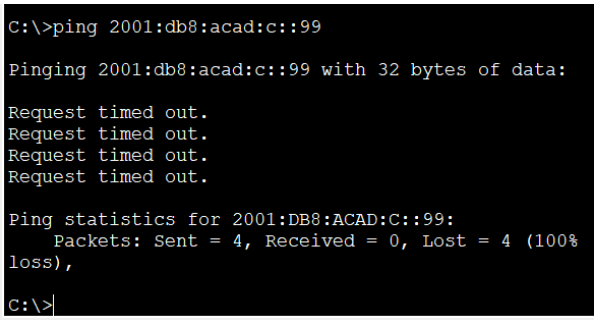
Fuente: Autor

Se evidencia ping exitoso entre el pc-b y la ipv6 2001:db8:acad:c::1 ya que se encuentra bien la configuración de extremo a extremo.</td></tr>
<tr><td>S1, VLAN 40</td><td>IPv4</td><td>10.12.8.98</td><td>Figura 32. Ping PC-B a 10.12.8.98
 

Fuente: Autor

Se encuentra satisfactorio ping desde el pc-b a la ip 10.12.8.98 ya que su configuración es excelente.</td></tr>
</table>

		IPv6	2001:db8:acad:c::98	Figura 33. Ping PC-B a 2001:db8:acad:c::98  Fuente: Autor El ping en este caso no es satisfactorio por un problema del IOS del switch, su configuración realizada en el escenario está correcta.
	S2, VLAN 40	IPv4	10.12.8.99	Figura 34. Ping PC-B a 10.12.8.99  Fuente: Autor Se evidencia ping exitoso entre el pc-b y la ip 10.12.8.99 ya que se encuentra exitoso de extremo a extremo.

		IPv6	2001:db8:acad:c::99	Figura 35. Ping PC-B a 2001:db8:acad:c::99  Fuente: Autor El ping en este caso no es satisfactorio por un problema del IOS del switch, su configuración realizada en el escenario está correcta.

Fuente: Autor

CONCLUSIONES

De acuerdo con la prueba de habilidades practica CCNA referenciado en los escenarios, se puede dilucidar la importancia de aplicar las habilidades necesarias respecto a la configuración de los diferentes componentes, la realización de la documentación requerida para contemplar los comandos necesarios en cada uno de los pasos y así poder reflejar el desarrollo de los diversos aspectos adquiridos a lo largo del diplomado.

De este modo, en los escenarios se establecen las diferentes fases el cual llevan a la creación de labores en donde se pueda incorporar, diseñar y configurar los diferentes equipos que se establezcan una seria de red y subredes, permitiendo identificar cada uno de los equipos por medio de un esquema de direccionamiento IP, realizando los diferentes ajustes necesarios con los ajustes básicos en seguridad para nuestros Router y Swich, el cual nos permita la conectividad entre cada uno de los equipos que conforman esta gran red.

Hay que tener en cuenta que al momento de la creación de nuestro esquema de direccionamiento se debe de verificar la cantidad de elementos el cual va a conformar nuestra red y la cantidad de elementos el cual se pueda conformar a futuro, ya que, si por alguna razón se desea incorporar otra impresora, router o pc esta pueda incluirse sobre nuestra red existente sin ningún problema.

REFERENCIAS BIBLIOGRÁFICAS

CARRIÓN, Amaya y ELSA Wendy. Introducción a las redes, necesidad de una red, tipo y equipos de redes, topología de una red, diseño de redes, instalación y administración de redes LAN. . [página web]. (2018) [Consultado el 21, noviembre, 2022], Disponible en Internet: < https://repositorio.une.edu.pe/handle/20.500.14039/4118 >

CASTILLO, Porturas y AUGUSTO, Noé. Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabif. Universidad de ciencias y humanidades. [página web]. (2019) [Consultado el 21, noviembre, 2022], Disponible en Internet: < https://repositorio.uch.edu.pe/handle/20.500.12872/419>.

CISCO. Asignación de direcciones IPv4. netacad [página web]. (2020). [Consultado el 22, septiembre, 2022]. Disponible en Internet: <https://contenthub.netacad.com/itn/11.0.1>.

CISCO. Configuración básica de switches y terminales. netacad [página web]. (2020). [Consultado el 23, septiembre, 2022]. Disponible en Internet: < https://contenthub.netacad.com/itn/2.0.1>.

CISCO. Configuración básica de un router.. netacad [página web]. (2020). [Consultado el 27, septiembre, 2022]. Disponible en Internet: < https://contenthub.netacad.com/itn/10.0.1>.

CISCO. Capa de red. netacad [página web]. (2020). [Consultado el 03, octubre, 2022]. Disponible en Internet: < https://contenthub.netacad.com/itn/8.0.1>.

CRUZ, Wilfredo. Subnetting. [página web]. [Consultado el 02, noviembre, 2022]. Disponible en Internet: < http://wcruzy.pe/tcpip/subnetting.pdf >.

ANEXOS

Anexo A. Descarga de archivos de simulación.

Enlace: https://drive.google.com/drive/folders/1ZOZX0UppXxC4YXCG-GCMD0ysya9VX0E9?usp=share_link