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

HAROLD VICENTE ORTEGA

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

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

HAROLD VICENTE ORTEGA

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

PAULITA FLOR
DIRECTORA:

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

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado.

_____

Firma del Jurado

_____

Firma del Jurado

PASTO, 22 de noviembre del 2022

AGRADECIMIENTOS

Le agradezco a la Universidad UNAD por todo eso compromiso con nosotros como estudiantes por ese compromiso por brindar una educación de calidad en modalidad a distancia, todo esto con el fin de podernos superar constantemente y formarnos como unas personas íntegras dentro de nuestras ramas del saber.

Agradecimientos especiales a los TUTORES por ser las personas que nos brindaron su conocimiento y toda su disponibilidad con el fin de superar las dificultades que constantemente se nos presentaba.

A todo el personal de la universidad que directa o indirectamente nos colaboraron para cumplir con nuestros quehaceres.

A todos mis compañeros por el compartir, aceptar y apoyar cada una de las actividades propuestas.

TABLA DE CONTENIDO

Contenido

Tabla de Figuras

Lista de Tablas.

GLOSARIO

DHCP:
El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como "**Dynamic Host Configuration Protocol**", es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados[1].

Gateway:
Una puerta de enlace es un nodo (router) en una red de computadoras, un punto clave de detención de datos en su camino hacia o desde otras redes. La dirección de la puerta de enlace (o **default gateway**) es una interfaz de router conectada a la red local que envía paquetes fuera de la red local[2].

IEEE 802.1Q
El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales[3].

Protocolos:
Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales[4].

[1] GOITIA, María Julieta. Protocolos de enrutamiento para la capa de red en arquitecturas de redes de datos. (2004).
[2] BANDYOPADHYAY, Soma; BHATTACHARYYA, Abhijan. Lightweight Internet protocols for web enablement of sensors using constrained gateway devices. (2013).
[3] THALER, Patricia. IEEE 802.1 Q. (2013).
[4] GOITIA, María Julieta. Protocolos de enrutamiento para la capa de red en arquitecturas de redes de datos. (2004).

VLAN:

Una V LAN (Virtual LAN) agrupa lógicamente dispositivos en un mismo dominio de broadcast, creando lógicamente distintas redes como si fueran distintas redes físicas5.

VLSM:

Las máscaras de subred de tamaño variablemente pequeño o VLSM (del inglés Variable Length Subnet Mask) representan otra de las tantas soluciones que se implementaron para evitar el agotamiento de direcciones IP en IPv4 (1987), como la división en subredes (1985), el enrutamiento sin clases (CIDR) (1993), NAT y las direcciones IP privadas[6].

[5] SINURAYA, Enda Wista. Teknik Variable Length Subnet Mask (Vlsm) Dan Virtual Local Area Network (Vlan). *(*2014).

[6] SINURAYA, Enda Wista. Teknik Variable Length Subnet Mask (Vlsm) Dan Virtual Local Area Network (Vlan). *(*2014).

RESUMEN

El desarrollo de esta actividad es de vital importancia como profesional, se van a desarrollar, documentar y configurar 2 redes las cuales tienen una serie de exigencias bien marcadas las cuales se debe cumplir como responsables del diseño de las mismas.

Para el primer caso ESCENARIO 1 se va a configurar una red pequeña en la cual se va a configurar los parámetros básicos dentro de cada uno de los dispositivos que hacen parte de la misma, la configuración se realizará de los routers, switches y PC, se configurará las contraseñas, interfaces y para el direccionamiento de la RED se aplicará VLSM con el fin de ajustar el diseño de la misma a las necesidades reales de la organización.

Para el caso del ESCENARIO 2 la red es un poco más compleja ya que se profundiza un poco más en aspectos muy importantes dentro del diseño de las redes, igualmente se realiza la configuración básica de cada uno de los dispositivos, contraseñas, interfaces, subinterfaces tanto aplicando direccionamiento IPV4 como IPV6 mediante VLSM. Algo nuevo que se configura en este ESCENARIO es lo relacionado con las VLAN aspecto que como se verá es vital con el fin de organizar y brindar seguridad a la red mejorando su rendimiento y eficiencia. Se realiza igualmente la configuración de DHCP en los routers, esto con el fin de brindar direcciones IPV4 de manera automática de algunas de sus VLAN.

Como vemos este trabajo permitirá practicar muchos de los temas tratados en el DIPLOMADO desarrollando diversas actitudes.

Se espera que este trabajo sea del agrado de todos ustedes.

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

ABSTRACT

The development of this activity is of vital importance as a professional, 2 networks will be developed, documented and configured, which have a series of well-defined requirements which must be met as those responsible for their design.

For the first case SCENARIO 1, a small network will be configured in which the basic parameters will be configured within each of the devices that are part of it, the configuration will be made of the routers, switches and PCs, configure the passwords, interfaces and for the addressing of the NETWORK, VLSM will be applied in order to adjust its design to the real needs of the organization.

In the case of SCENARIO 2, the network is a little more complex since it goes deeper into very important aspects within the design of the networks, the basic configuration of each of the devices, passwords, interfaces, subinterfaces, both applying IPV4 as IPV6 addressing via VLSM. Something new that is configured in this SCENARIO is related to VLANs, an aspect that, as will be seen, is vital in order to organize and provide security to the network, improving its performance and efficiency. The DHCP configuration is also carried out on the routers, in order to automatically provide IPV4 addresses for some of their VLANs.

As we can see, this work will allow practicing many of the topics covered in the DIPLOMA, developing different attitudes.

It is hoped that this work will be to the liking of all of you.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics.

INTRODUCCION

La humanidad está inmersa en un periodo de mucho cambio y el cambio se hace de una manera muy rápida, hay muchos avances tecnológicos en todos los campos, pues independiente del área en el cual nos desenvolvamos se depende directa o indirectamente de estas tecnologías.

Las telecomunicaciones han sido uno de los aspectos que más han evolucionado, es una necesidad el hecho de permanecer conectados y de mantener la información a nuestro alcance. Empresas pequeñas, medianas o grandes pueden crecer rápidamente siempre y cuando utilicen los medios adecuados para mantenerse conectado con sus clientes y podamos emplear de manera adecuada la información con la que se dispone.

Se ve entonces que es muy importante el hecho de que dentro de nuestra formación profesional se tenga un amplio conocimiento acerca de las redes de datos, y que mejor manera que podamos afianzar y mejorarlos a través de una práctica de estos 2 ESCENARIOS que muy seguramente se podrá encontrar en la vida profesional. Este trabajo va a permitir familiarizarnos mucho con todos los dispositivos que intervienen en una red, permitiendo diferenciar entre sus posibilidades, ventajas y desventajas y sus aplicaciones dependiendo de las exigencias que se presentan.

Para finalizar se indica que el montaje de la red se realizó dentro del simulador, magnífica herramienta desarrollada por CISCO, llamada PACKET TRACER, gracias a este se puede ejecutar gran parte de los comandos que se pueden configurar dentro de los dispositivos reales.

1. DESARROLLO ESCENARIO 1.

En esta primera actividad se configuran los dispositivos que hacen parte de esta pequeña red, se diseñará el respectivo direccionamiento IP siguiendo las necesidades que se nos muestra.

1.1 Topología Escenario 1.

Figura 1. Topología escenario 1

Fuente: Autor.

Para este escenario 1, como vemos en la Figura 1. Se realizará la configuración de Switches, Routers y PC. De acuerdo a las exigencias de las redes se realizará el esquema de direccionamiento aplicando VLSM con el fin de ajustar el mismo a las necesidades de lo solicitado, Para la LAN1 (60 host) y la LAN2 (20 hosts).

1.2 Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cableeconforme se indica en la topología, y conecte los equipos de cómputo

Figura 2: Topología en Packet Tracer.

Fuente: Autor.

1.3 Desarrolle el esquema de direccionamiento IP

Cada estudiante tomará el direccionamiento **172.68.3.0** donde XY corresponde a los últimos dos dígitos desu cédula.

Se nos entrega el rango IP indicado antes con el cual debemos configurar las dos subredes LAN supliendo los requisitos indicados para cada una de ellas.

Subneteo del rango IP:

Lo primero que debemos hacer en el caso de que conocemos la TOPOLOGÍA con los requisitos de cada una de las subredes es proceder a Subneteo el rango asignado, el mismo nos queda de la siguiente manera:

La red en general está formada por 2 subredes:

Tabla 1. Asignación de subredes.

RED	N° IP	DIR RED	MASC	/	BROADCAST	DISPONIBLES
LAN 1	60	172.68.3.0	255.255.255.192	26	172.68.3.63	62
LAN 2	20	172.68.3.64	255.255.255.224	27	172.68.3.95	30

Fuente: Autor.

Figura 2. Rango IP LAN 1.

IP Address:	172.68.3.0
Network Address:	172.68.3.0
Usable Host IP Range:	172.68.3.1 - 172.68.3.62
Broadcast Address:	172.68.3.63
Total Number of Hosts:	64
Number of Usable Hosts:	62
Subnet Mask:	255.255.255.192
Wildcard Mask:	0.0.0.63
Binary Subnet Mask:	11111111.11111111.11111111.11000000
IP Class:	C
CIDR Notation:	/26
IP Type:	Public

Fuente: Autor.

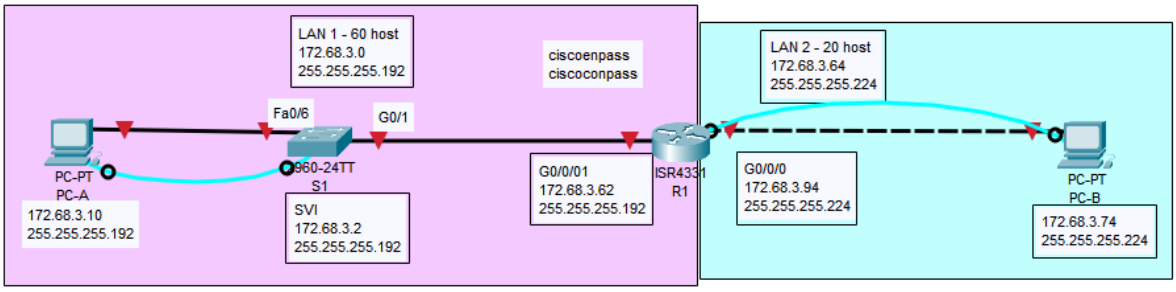
Figura 3. Rango IP LAN 2.

IP Address:	172.68.3.64
Network Address:	172.68.3.64
Usable Host IP Range:	172.68.3.65 - 172.68.3.94
Broadcast Address:	172.68.3.95
Total Number of Hosts:	32
Number of Usable Hosts:	30
Subnet Mask:	255.255.255.224
Wildcard Mask:	0.0.0.31
Binary Subnet Mask:	11111111.11111111.11111111.11100000
IP Class:	C
CIDR Notation:	/27
IP Type:	Public

Fuente: Autor.

Como ya conocemos los rangos IP para cada una de las subredes podemos proceder a realizar la asignación de la IP correspondiente a cada una de las interfaces que intervienen, este queda como se indica a continuación:

Figura 4. Topología ESCENARIO 1 con direcciones IP.



Fuente: Autor.

Como ya conocemos los diferentes rangos que se deben asignar a cada una de las LAN de la red podemos ya en este punto proceder a realizar la asignación de la dirección IP a cada una de las interfaces de los dispositivos que intervienen, tanto Routers, Switches, PC.

1.4 Tabla de direccionamiento

Tabla 2. configuración básica y asignación de direcciones IP.

Item	Requerimiento
Dirección de Red	La dirección IP 172.68.3.0 es con la cual voy a cumplir los requerimientos de direccionamiento de la red en general.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1. Para esta interfaz la debemos configurar como se indica a continuación: Int g0/0/1 Ip address 172.68.3.62 255.255.255.192
R1 G0/0/0	Última dirección de host de la subred LAN2. Igualmente, esta interface se configuración aplicando el siguiente comendo: Int g0/0/0 Ip addres 172.68.3.94 255.255.255.224
S1 SVI	Segunda dirección de host de la subred LAN1. Para éste switch la configuración la debemos hacer como se muestra:

	Int vlan 1 Ip address 172.68.3.2 255.255.255.192
PC-A	Décima dirección de host de la subred LAN1 Ya para configurar las interfaces NIC de los PC debemos ingresar en la PC-A la siguiente dirección: IP: 172.68.3.10 Mask: 255.255.255.192
PC-B	Décima dirección de host de la subred LAN2 Ya para configurar las interfaces NIC de los PC debemos ingresar en la PC-B la siguiente dirección: IP: 172.68.3.74 Mask: 255.255.255.224

Fuente: Cisco.

1.5 Configure aspectos básicos

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

Comenzamos nuestro proceso de configuración con el Router R1, en esta primera parte los parámetros básicos del mismo.

Como siguiente paso se procede a realizar la configuración básica de R1 con el fin de agregar seguridad al mismo y poder configurar sus interfaces, el proceso es indicado a continuación:

Tabla 3. Configuración básica R1.

Tarea	**Especificación**
Desactivar la búsqueda DNS	Se desactiva la búsqueda de DNS con el fin de ahorrar recursos necesarios dentro de

	nuestra red, estala aplicamos en R1. No ip domain lookup.
Nombre del router	Debemos hacer este proceso con el fin de poder identificar nuestros dispositivos de una manera sencilla. hostname R1.
Nombre de dominio	ccna-sa.com ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Debemos cifrar nuestras contraseñas: Ciscoenpass enable secret ciscoenpass
Contraseña de acceso a la consola	Debemos proteger este puerto, ya que debemos recordar que es solo conectar y utilizar, no podemos dejar nuestros dispositivos desprotegidos. Procedemos a configurar nuestras lineas de consola empleando la contraseña: Ciscoconpass line console 0 password ciscoconpass login
Establecer la longitud mínima para las contraseñas	Este comando lo aplicamos con el fin de exigir contraseñas seguras o con un tamaño determinado, para nuestro caso la exigencia es que tenga como mínimo de 10 caracteres: security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**

	username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Procedemos a configurar las líneas vty 0 15 line vty 0 15 login local
Configurar VTY solo aceptando SSH	transport input ssh login
Cifrar las contraseñas de texto no cifrado	De esta manera logramos que las contraseñas permanezcan encriptadas y que permanezcan ocultas. Service password-encyption
Configure un MOTD Banner	Configuramos el mensaje de bienvenida el cual tiene muchos fines cuando se configura: banner motd % Se prohíbe el acceso no autorizado. %
Configurar interfaz G0/0/0	En este nuevo paso lo que debemos hacer es configurar la interface de acuerdo a la dirección IP que le hemos asignado dentro del diagrama. Demos recordar que todas las interfaces se deben activar Config t Int g0/0/0 Ip address 172.68.3.94 255.255.255.224.
Configurar interfaz G0/0/1	En este nuevo paso lo que debemos hacer es configurar la interface de acuerdo a la dirección IP que le hemos asignado dentro del diagrama. Demos recordar que todas las interfaces se deben activar Configure t Interface g0/0/01 Ip address 172.68.3.62 255.255.255.192

Generar una clave de cifrado RSA	Módulo de 1024 bits crypto key generate rsa general-keys modulus 1024

Fuente: Cisco.

Verificamos a ingresar la configuración del dispositivo tal como se muestra a continuación:

```
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#ip domain-name ccna-sa.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#username admin secret admin1pass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#banner motd %prohibido el acceso no autorizado%
R1(config)#do wr
```

Procedemos a realizar la configuración de las interfaces de este dispositivo:

```
R1(config)#int g0/0/1
R1(config-if)#ip address 172.68.3.62 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#int g0/0/0
R1(config-if)#ip address 172.68.3.94 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#
R1(config)#crypto key generate rsa general-keys modulus 1024
```

1.6 Las tareas de configuración de <u>S1</u> incluyen lo siguiente:

Tabla 4. Configuración básica S1.

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Desactivamos la búsqueda de DNS esto con el fin de ahorrar recursos. No ip domain lookup
Nombre del switch	Esta es una opción muy importante, ya que es la forma como podemos identificar a nuestros dispositivos. hostname S1
Nombre de dominio	**ccna-sa.com** ip domain-name **ccna-sa.com**
Contraseña cifrada para el modo EXEC privilegiado	Creamos la contraseña de EXCEC privilegiado y la ciframos Ciscoenpass enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** line console 0 password ciscoconpass login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local	line vty 0 15 login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	Este comando nos sirve para cifrar todas las contraseñas que aún no lo han hecho.

	Service password-encyption
Configurar un MOTD Banner	Configuramos el mensaje que aparece en el dispositivo cuando ingresamos al mismo: banner motd % Se prohíbe el acceso no autorizado.%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Procedemos a configurar la dirección IP para la interface VLAN 1. int vlan 1 description subnet A ip address 172.68.3.2 255.255.255.192
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla dedireccionamiento. ip default-gateway 172.68.3.62

Fuente: Cisco.

Procedemos a realizar la configuración básica del dispositivo S1, tal como se indica en la tabla anterior:

Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#ip domain-name ccna-sa.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config)#service password-encryption

S1(config)#banner motd %prohibido acceso sin autorizacin%
S1(config)#crypto key generate rsa general-keys modulus 1024

Procedemos a realizar la de las interfaces del S1:

S1(config)#int vlan 1
S1(config-if)#description subnet A
S1(config-if)#ip address 172.68.3.2 255.255.255.192
S1(config-if)#ip default-gateway 172.68.3.62
S1(config)#do wr

1.7 Configurar los equipos PC.

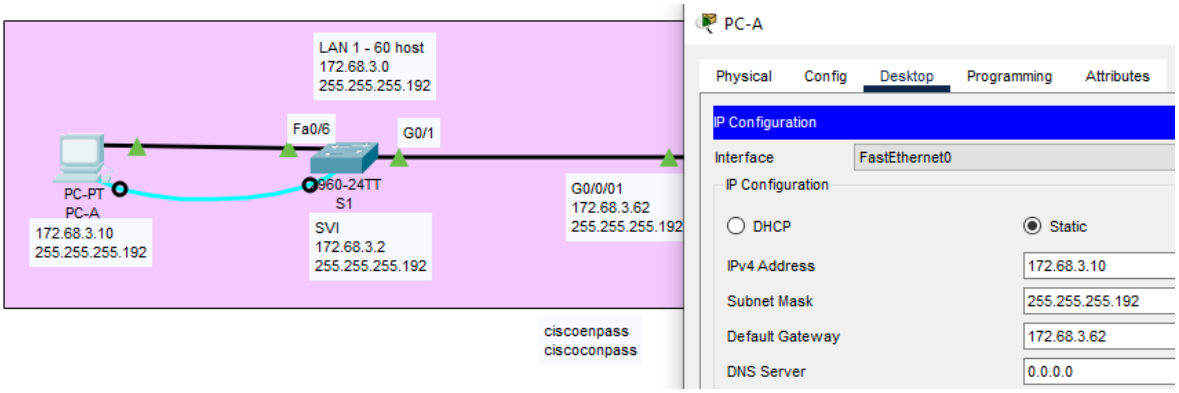
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 5. Configuración PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	
Dirección IP	172.68.3.10
Máscara de subred	255.255.255.192
Gateway predeterminado	172.68.3.62

Fuente: Cisco - Autor.

Figura 5. configuración PC-A



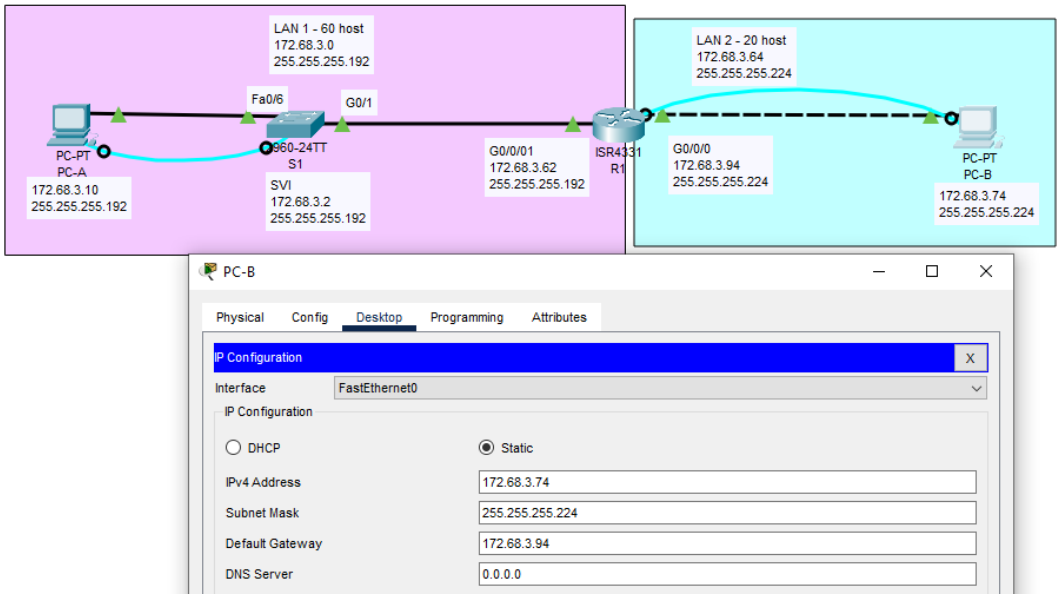
Fuente: Autor.

Tabla 6. Configuración PC-B

PC-B Network Configuration	
Descripción	PC-B
Dirección física	
Dirección IP	172.68.3.74
Máscara de subred	255.255.255.224
Gateway predeterminado	172.68.3.94

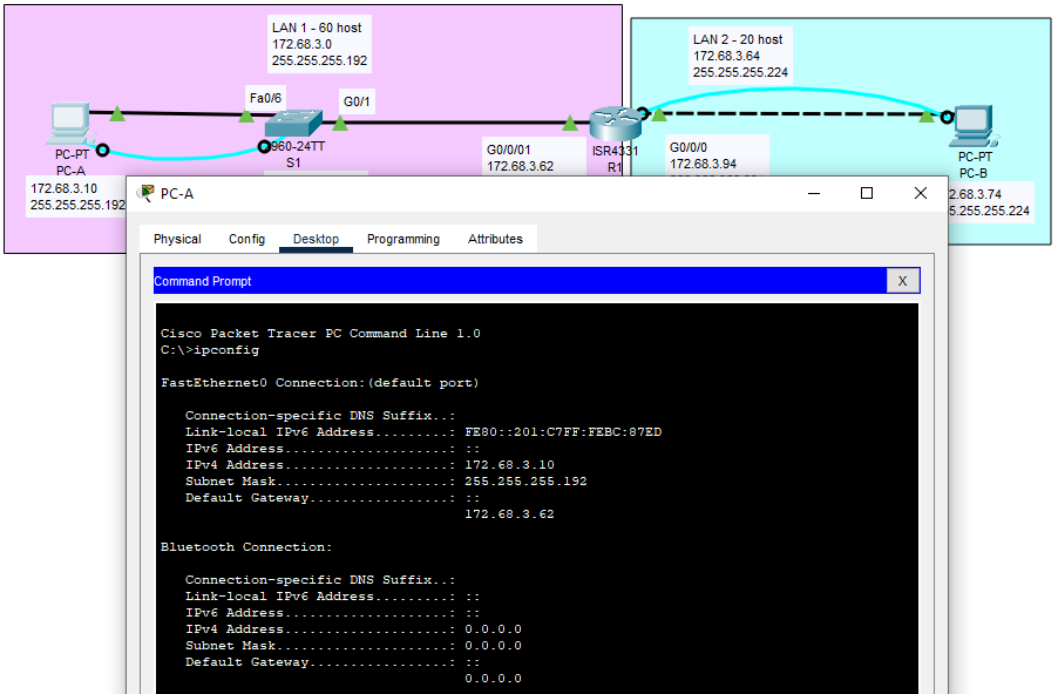
Fuente: Cisco - Autor.

Figura 6. Configuración PC-B



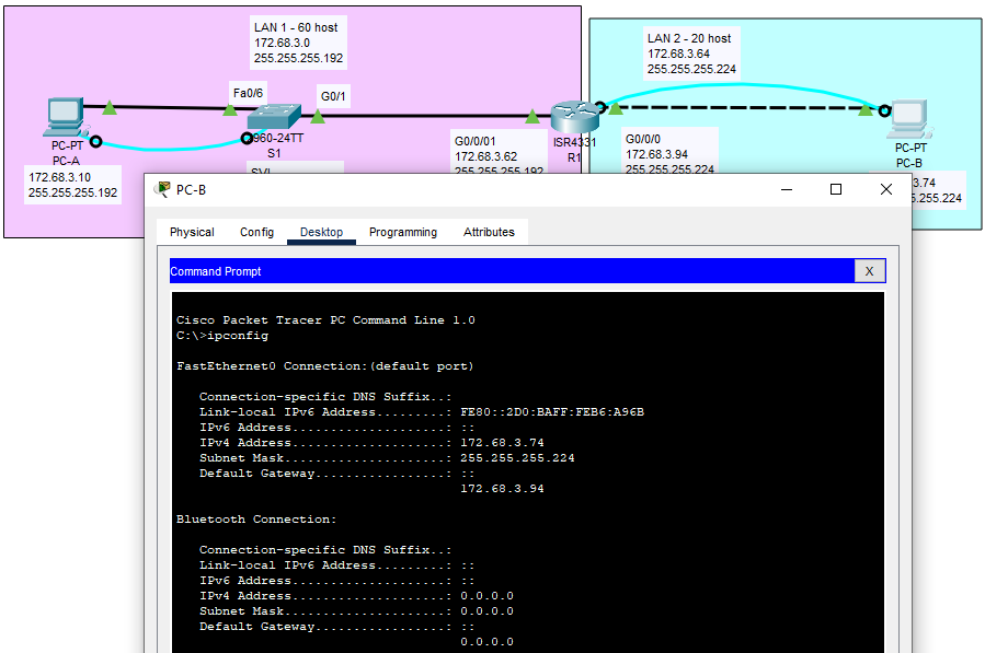
Fuente: Autor.

Figura 7. MAC PC-A



Fuente: Autor.

Figura 8. Dirección MAC - PCB



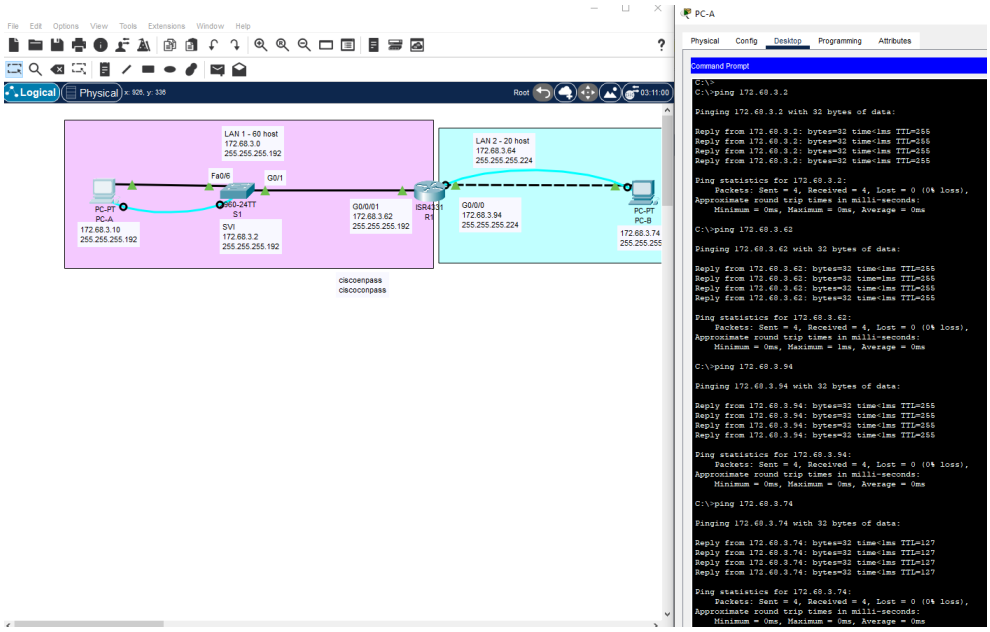
Fuente: Autor.

1.8 Pruebas de Conectividad Escenario 1.

Desde PCA hacia los diferentes puertos de la red.

Como se observa en la Figura 9, si hacemos PING desde la PCA hacia los diferentes puntos de la red se observa que estos son satisfactorios, con lo cual se concluye que este dispositivo cuenta con una ruta para cada uno de los puntos de la red y que nuestra red es convergente.

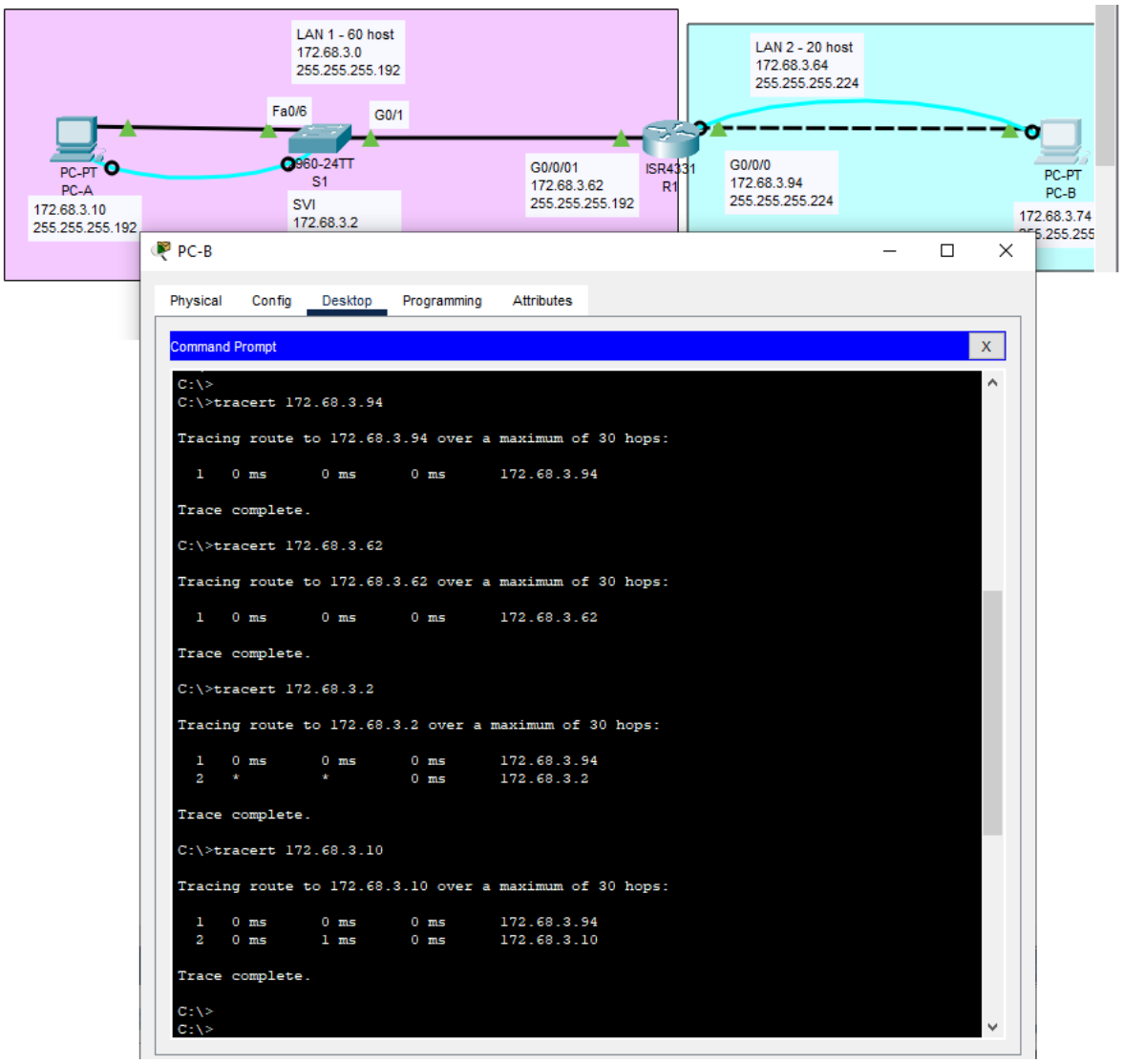
Figura 9. PING desde el PC-A



Fuente: Autor.

Procedemos a realizar la verificación de lo hecho hasta el momento, para nuestro caso vamos a emplear el comando TRACERT esta vez desde la PC-B tal como se puede observar en la Figura 10, hacia los diferentes puntos de la red.

Figura 10. Comando TRACERT desde PCB.



Fuente: Autor.

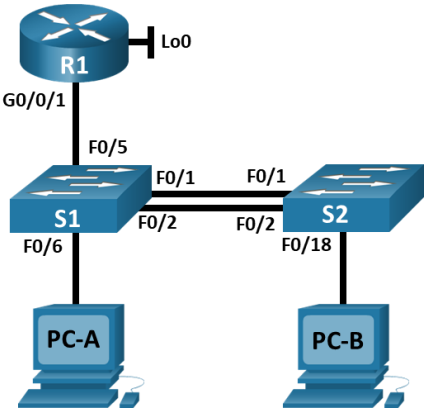
Se verifica igualmente que la red cuenta con rutas para cada uno de los puntos de la misma ya que obtenemos respuesta, se concluye que la red es convergente.

2. DESARROLLO ESCENARIO 2.

Se procede ahora a realizar el diseño y configuración de los diferentes dispositivos que hacen parte del ESCENARIO 2, escenario que cuenta con 2 switches, 1 Router y PC.

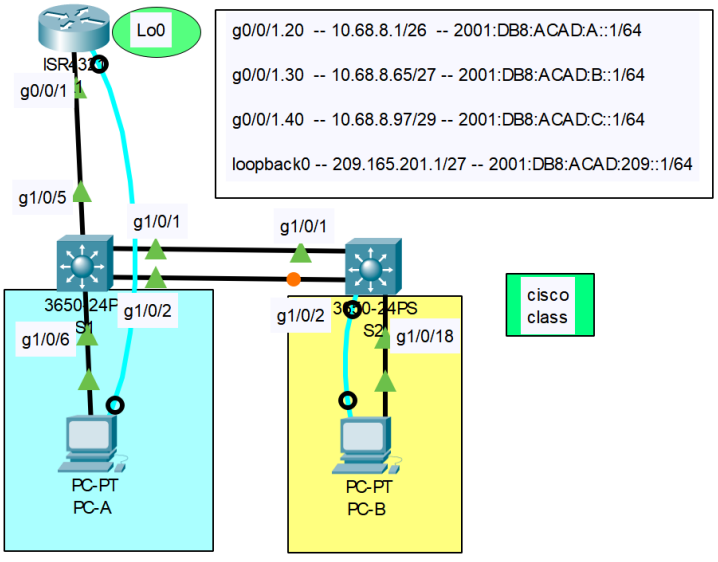
2.1 Topología

Figura 11. Topología propuesta escenario 1



Fuente: Autor

Figura 12. Topología desarrollada escenario 1



Fuente: Autor

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

Tabla 7. Nombre VLAN -Escenario 1

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

Fuente: Cisco.

2.2 Tabla de asignación de direcciones

Tabla 8. Asignación de direcciones IP

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.68.8.1 /26	No corresponde
R1 G0/0/1.20	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.68.8.65 /27	No corresponde
R1 G0/0/1.30	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.68.8.97 /29	No corresponde
R1 G0/0/1.40	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
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 40	10.68.8.98 /29	10.68.8.97
VLAN S1 40	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 40	fe80: :98	No corresponde
S2 VLAN 40	10.68.8.99 /29	10.68.8.97
S2 VLAN 40	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 40	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Cisco.

2.3 Inicializar y volver a cargar el router y el switch

Este proceso con el fin de asegurarnos de que no hay ningún tipo de configuración dentro de los dispositivos que pueda crear algún tipo de conflicto con la configuración que se va a ingresar ahora.

S1
Erase startup-config
Delete vlan.dat
Reload

S2
Erase startup-config
Delete vlan.dat
Reload

El proceso que se muestra con la ejecución de los comandos anteriores, se debe ejecutar tanto en los dos Switch como también en el Router.

Recordemos que los dispositivos prácticamente están en blanco, por lo cual podemos proceder a configurar las plantillas SDM.

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario. Por ultimo no olvidemos que debemos volver a cargar el switch.

  Show sdm prefer
  Vemos que soporta IPV6
  Sdm prefer dual-ipv4

2.4 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Como objetivo principal de este paso es ajustar a los dispositivos para que sean accesibles y además poderles brindar seguridad. incluyendo un password, si no se conoce la contraseña de acceso aparecerá el mensaje de acceso no permitido, sirviendo esto como método disuasivo para usuarios no autorizados. Se asigna tanto direccionamiento ipv4 e ipv6 y se configura las respectivas troncales, y para finalizar nuestro proceso lo que hacemos es generar una clave segura y además la encriptamos.

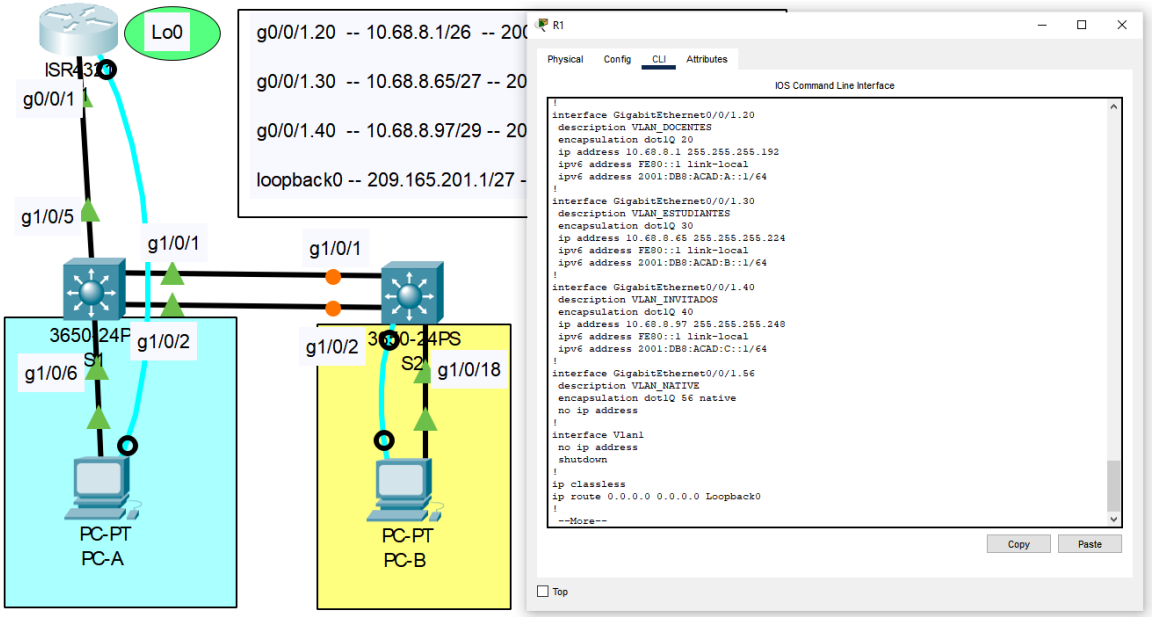
Tabla 9. Configuración R1- Escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ccna-sa.com ip domain-ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Class Enable secret class
Contraseña de acceso a la consola	Cisco Line console 0 Password cisco Login
Establecer la longitud mínima para las contraseñas	5 caracteres Security passwords min-leng 5
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vt 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configure un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Habilitar el routing IPv6	Ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz. **Int g0/0/1.20** Encapsulation dot1q 20 Description DOCENTES Ip addres 10.68.8.1 255.255.255.192

Tarea	Especificación
	Ipv6 addres 2001:db8:acad:a:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1.30** Encapsulation dot1q 30 Description ESTUDIANTES Ip addres 10.68.8.65 255.255.255.224 Ipv6 addres 2001:db8:acad:b:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1.40** Encapsulation dot1q 40 Description INVITADOS Ip addres 10.68.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1.56** Encapsulation dot1q 56 NATIVE Description NATIVE Ip addres 10.68.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local **Int g0/0/1** No shutdown
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1** Interface loopback 0 Ip address 209.165.201.1 255.255.255.224 Ipv6 address 2001:db8:acad:209::1/64 Ipv6 address fe80::1 link-local Description SALIDA INTERNET
Generar una clave de cifrado RSA	Módulo de 1024 bits Crypto key generate rsa modulus 1024

Fuente: Cisco - Autor.

Figura 13. Show running-config: verificación subinterfaces.



Fuente: autor.

2.5 Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Comenzamos realizando la configuración de los 2 switches, los comandos que vamos a aplicar son los más básicos, comenzaremos configurando los respectivos nombres de cada uno de los dispositivos, desactivamos la búsqueda DNS aplicando el comando “NO IP DOMAIN LOOKUP” con lo cual evitamos la traducción de nombres a direcciones IP, configuramos todo lo relacionado a las VLAN, junto con sus enlaces TRONCALES, y por último debemos proceder a agregar contraseñas tanto a la línea de consola líneas VTY, y los mensajes BANNER MOTD, mensaje que aparecen cada vez que ingresamos a los dispositivos.

Tabla 10. Configuración S1-S2 - Escenario 1

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S1 Hostname S2
Nombre de dominio	**ccna-lab.com**

Tarea	Especificación
	ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Class** Enable secret class
Contraseña de acceso a la consola	**Cisco** Line console 0 Password cisco Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa mosulus 10242
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 Int vlan 40 Ip address 10.68.8.98 255.255.255.248 Ipv6 address 2001:db8:acad:c::98/64 Ipv6 address fe80::98 link-local Description ADMINISTRACIÓN

Tarea	Especificación
	No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.68.8.97 para IPv4 Ip Default-gateway 10.68.8.97

Fuente: Cisco - Autor.

2.6 Configure S2

Las tareas de configuración incluyen lo siguiente:

Tabla 11. Configuración S1-S2 - Escenario 2

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S2
Nombre de dominio	**ccna-sa.com** ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	**class** Enable secret class
Contraseña de acceso a la consola	**Cisco** Line console 0 Password cisco Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd % Prohibido el acceso no autorizado %

Tarea	Especificación
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa modulus 1024 Crypto key generate rsa 1024
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 Int vlan 40 Ip address 10.68.8.99 255.255.255.248 Ipv6 address 2001:db8:acad:c::99/64 Ipv6 address fe80::99 link-local Description ADMINISTRACIÓN No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.68.8.97 para IPv4 Ip Default-gateway 10.68.8.97

Fuente: Cisco - Autor.

2.7 procedemos a realizar con configuración de aspectos muy importantes como lo son (VLAN, Trunking, EtherChannel)

2.7.1 Configurar S1

Ya dentro de esta nueva sección lo que se hace es dividir nuestra red general en subredes de manera lógica, este procedimiento lo conocemos con VLAN, este proceso nos va a mejorar el rendimiento de nuestra red, ya que lo que se hace es segmentar la misma en secciones dependiendo de nuestras necesidades lo que se verá reflejado en una mayor eficiencia. El Router es el encargado de lograr la comunicación de las VLAN a través de la configuración de enlaces TRONCALES los cuales serán los encargados de permitir el paso de los mensajes provenientes

de las diferentes subinterfaces. Para esta tarea se emplea un protocolo muy conocido IEEE 802.1Q, el cual lleva los paquetes a la VLAN especifica.

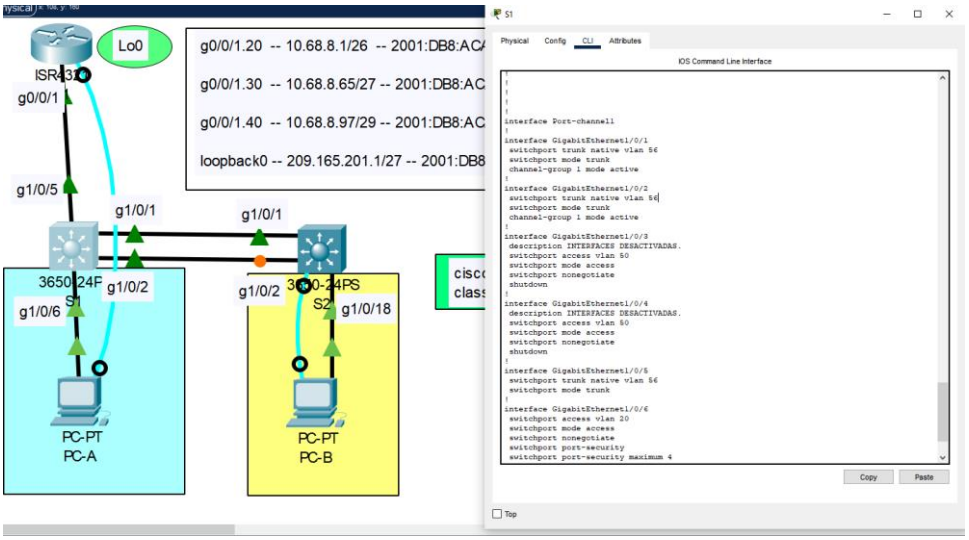
Tabla 12. Configuración S1-S2 - Escenario 2

Tarea	Especificación
Crear VLAN	Antes que nada, debemos crear las VLAN con las cuales vamos a trabajar, para mi caso iniciamos en el S1, Luego de crearlas debemos agregarles un nombre, de esta manera la podemos identificar facilmente. Vlan 20 Name DOCENTES Vlan 30 Name ESTUDIANTES Vlan 40 Name INVITADOS Vlan 50 Name USUARIOS Vlan 56 Name NATIVE
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Configuramos los enlaces por donde se va a comunicar mas de 1 VLAN como TRONCAL, este proceso queda de la siguiente manera: **Interface G1/0/5** Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 56 **Inteface range G1/0/1-2** Shutdown Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 56

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** Channel-group 1 mode active Int port channel 1 Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 56
Configurar el puerto de acceso de host para VLAN 20	Interface g1/0/6 Switchport mode access Switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC Switchport port-security máximum 4
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar **Int range g1/0/3-4** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown **Int range g1/0/7-24** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown **Int range g1/1/1-4** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown

Fuente: Cisco - Autor.

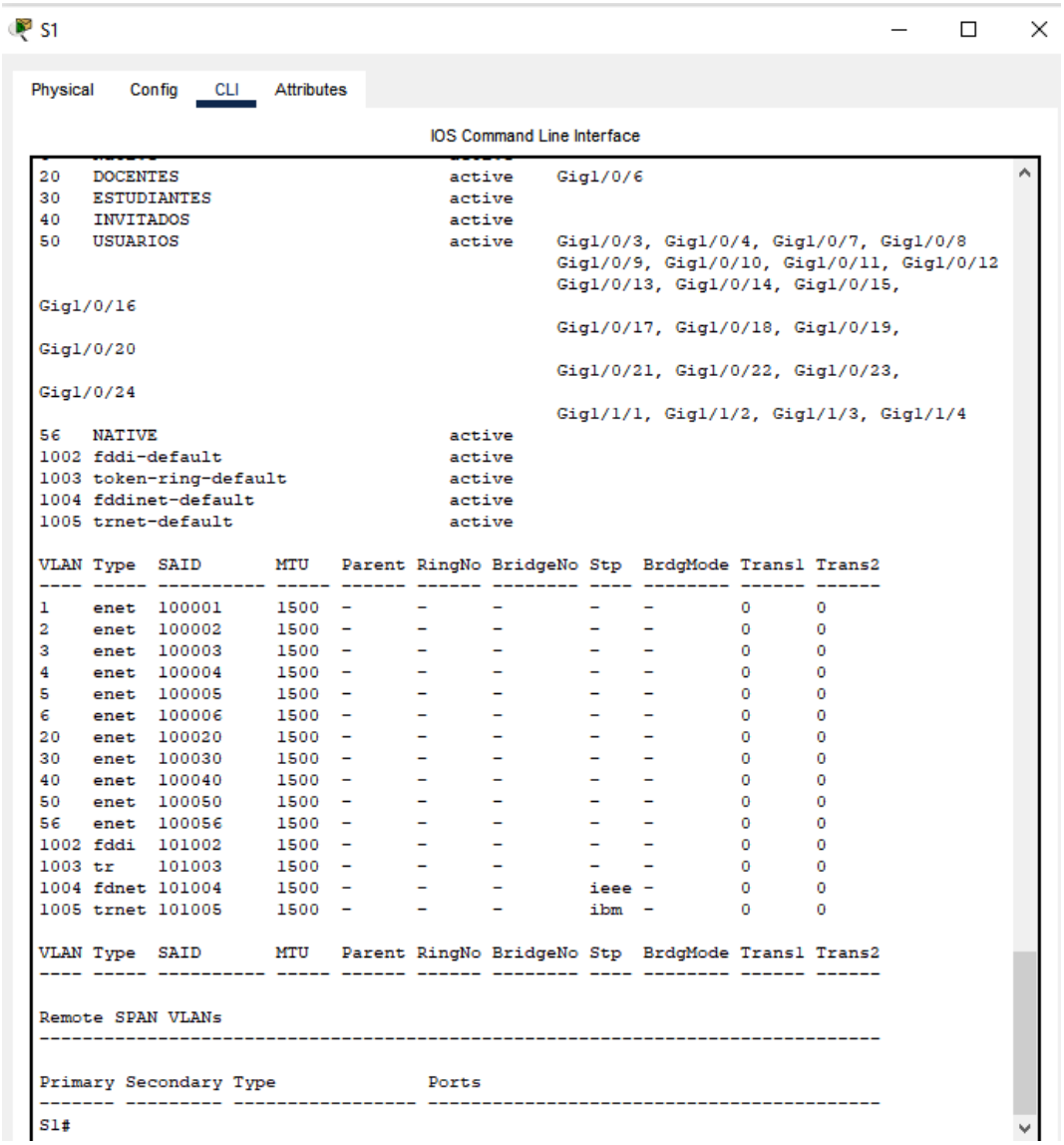
Figura 14. show running-configS1, verificación config R1.



Fuente: autor.

En el resultado anterior se puede constatar que cada uno de los pasos hechos en la fase anterior son correctos, cada interface y subinterfaces están configurados de manera adecuada y que las interfaces configuradas como TRONCALES también lo están. La asignación de las INTERFACES a las respectivas VLAN es correcta.

Figura 15. configuración S1, verificación de las VLAN.



Fuente: Autor

Mediante la utilización de este comendo observamos que las VLAN que configuramos dentro de S1 esta funcionando y que se crearon correctamente como se observa en la Figura 15.

2.7.2 Configure el S2.

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

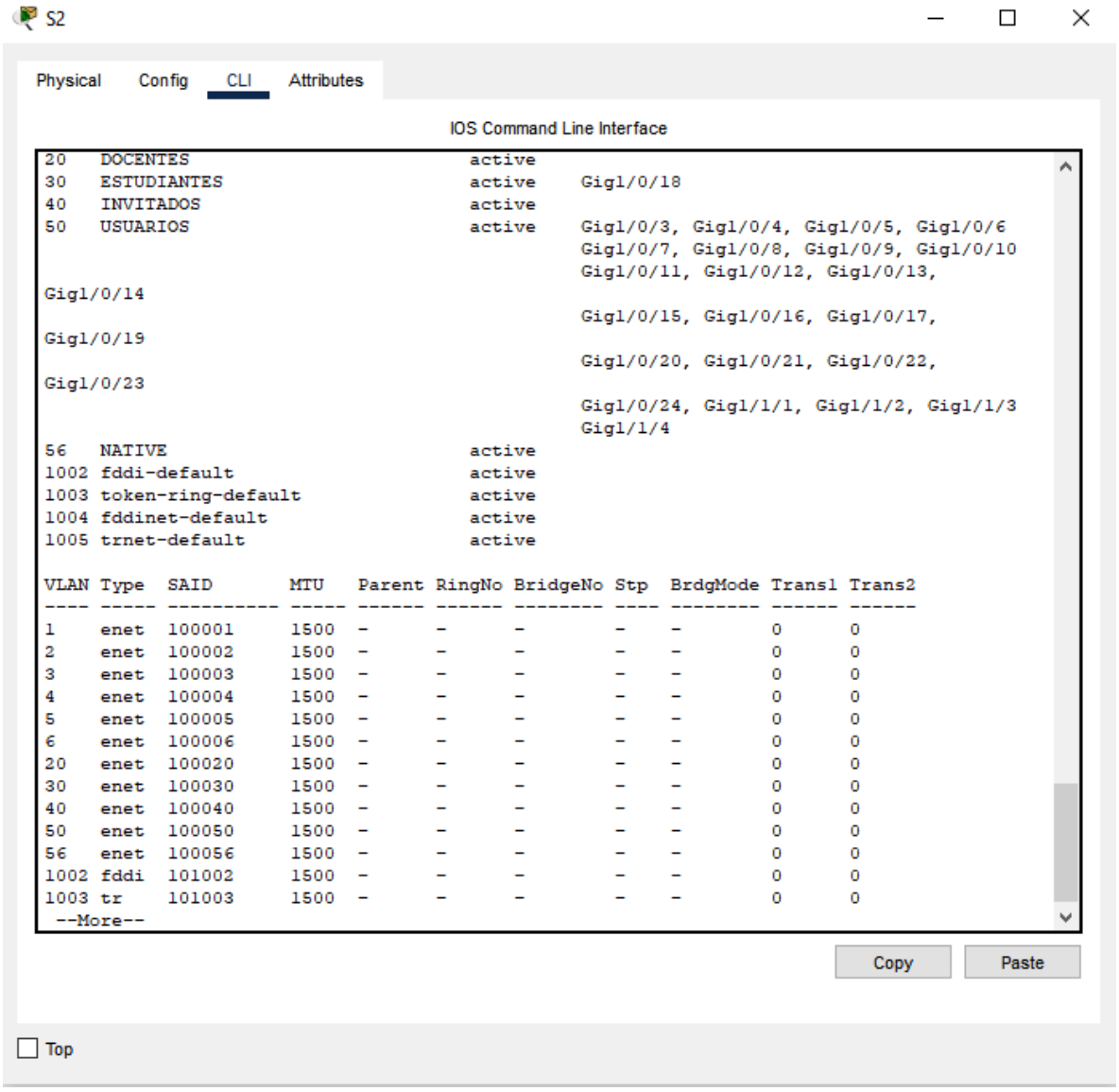
Tabla 13. Configuración S2 - Escenario 2

Tarea	Especificación
Crear VLAN	Antes que nada, debemos crear las VLAN con las cuales vamos a trabajar, para mi caso iniciamos en el S1, Luego de crearlas debemos agregarles un nombre, de esta manera la podemos identificar facilmente. Vlan 20 Name DOCENTES Vlan 30 Name ESTUDIANTES Vlan 40 Name INVITADOS Vlan 50 Name USUARIOS Vlan 56 Name NATIVE
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Configuramos los enlaces por donde se va a comunicar más de 1 VLAN, estos enlaces lo debemos configurar como TRONCAL, este proceso queda de la siguiente manera: Interfaces range G1/0/1-2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Channel-group 1 mode active Int port channel 1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 56

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 30	Interfaz F0/18 Int g0/1/18 Switchport mode Access Switchport Access vlan 30
Configure port-security en los access ports	permite 4 MAC addresses switchport port-security switchport port-security maximum 4
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar **Int range g1/0/3-17** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown **Int range g1/0/19-24** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown **Int range g1/1/1-4** Switchport mode Access Switchport Access vlan 50 Description INTERFACES DESACTIVADAS. Shutdown
Debemos activar las interfaces del etherchannel de cada uno de los 2 switches.	S1: G1/0/1-2 no shutdown S2: G1/0/1-2 no shutdown

Fuente: Cisco - Autor.

Figura 16. Configuración S2, verificación de las VLAN.



Fuente: Autor

Mediante la utilización de este comendo observamos que las VLAN que configuramos dentro de S2 está funcionando y que se crearon correctamente como se observa en la Figura 16.

2.7.3 Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

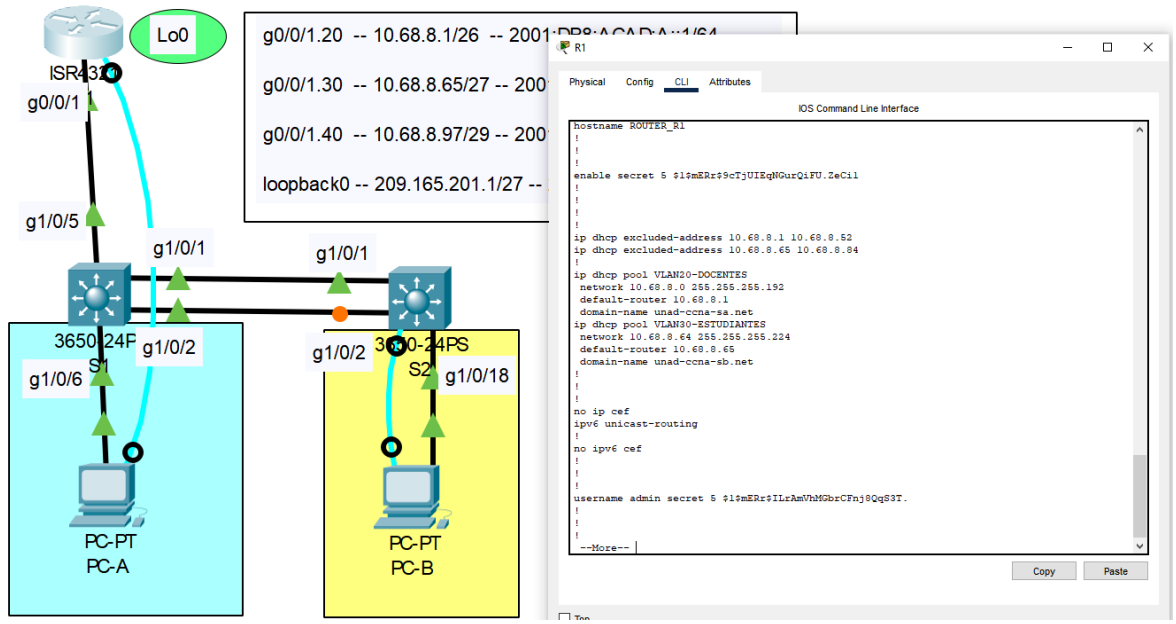
Tabla 14. Configuración R1 - Escenario 2

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e Ipv6 que dirijan el tráfico a la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 Ipv6 route ::/0 loopback 0
configurar IPv4 DHCP para VLAN 20	Cree un grupo DHCP para VLAN 20, compuesto por las **últimas 10 direcciones** de la subred solamente. Asigne el nombre de dominio ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada La red que se me ha asignado para esta SUBRED VLAN 20: 10.68.8.0 /26 El rango de direcciones utilizables es: 10.68.8.1 - 10.68.8.62 Recordemos que se nos pide que debemos trabajar con las 10 ultimas direcciones IP utilizables, entonces lo que hacemos es restringir las primeras. 10.68.8.1 - 10.68.8.52 estas serían las direcciones IP que se van a restringir empleando el siguiente comando: Ip dhcp excluded-address 10.68.8.1 10.68.8.52 Debemos entonces crear el POOL desde: 10.68.8.52 - 10.68.8.62 Ip dhcp excluded-address 10.68.8.1 10.68.8.52 Ip dhcp POOL VLAN20-DOCENTES Network 10.68.8.0 255.255.255.192 Default-route 10.68.8.1 Domain-name ccna-sa.net

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e Ipv6 que dirijan el tráfico a la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 Ipv6 route ::/0 loopback 0
Configurar DHCP IPv4 para VLAN 30	Cree un grupo DHCP para VLAN 30 ESTUDIANTES, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Para esta subred VLAN 30 se no asigno el rango: 10.68.8.64 /27 El rango IP de direcciones utilizables es: 10.68.8.65 - 10.68.8.94 Entonces, hacemos el mismo proceso que en el caso anterior, debemos restringir las primeras direcciones IP y solo dejar las que vamos a utilizar las 10 últimas del mismo. 10.68.8.65 - 10.68.8.84 este sería el rango que se va a restringir y con las otras es las que debemos emplear para DHCP. Debemos entonces crear el POOL desde: 10.68.8.85 - 10.68.8.94 Ip dhcp excluded-address 10.68.8.65 10.68.8.84 Ip dhcp POOL VLAN30-ESTUDIANTES Network 10.68.8.64 255.255.255.224 Default-route 10.68.8.65 Domain-name ccna-sb.net

Fuente: Cisco - Autor.

Figura 17. Configuración R1 escenario 2



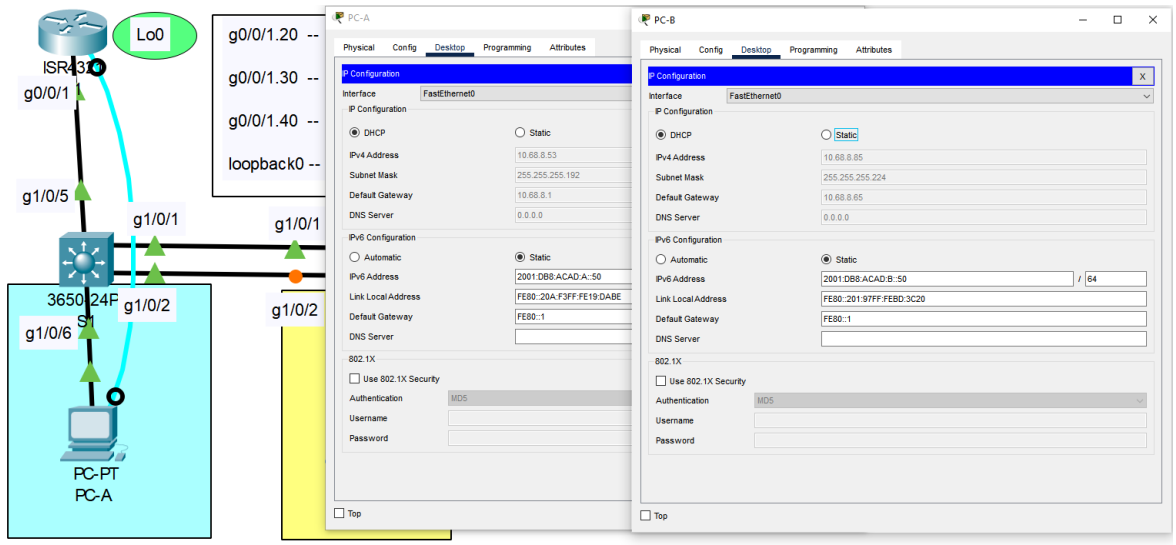
Fuente: Autor

Se observa que la configuración de las restricciones y del POOL de direcciones para DHCP se hizo de correctamente junto con las respectivas asignaciones de puerta de enlace predeterminado y el dominio.

2.7.4 Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Figura 18. Configuración PCA - PCB escenario 2



Fuente: Autor

En la Figura 18 observamos que la configuración del Servidor DHCP es correcta, ya que los PC toman la IP adecuada según lo que configuramos anteriormente.

Tabla 15. Configuración PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	
Dirección IP	10.68.9.53
Máscara de subred	255.255.255.224
Gateway predeterminado	10.68.8.1
Gateway predeterminado IPv6	FE80::1

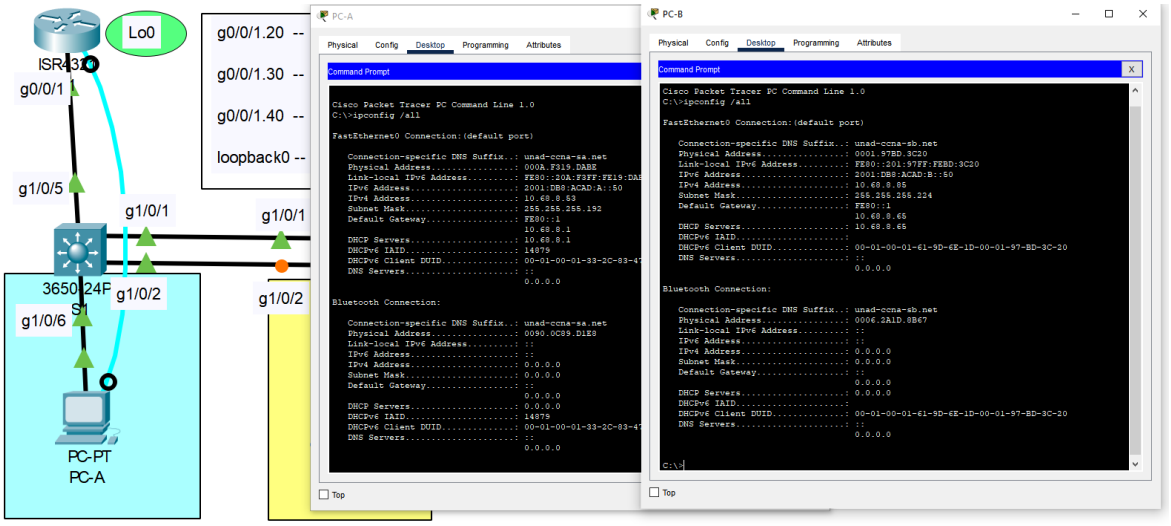
Fuente: Cisco - Autor.

Tabla 16. Configuración PC-B.

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	
Dirección IP	10.68.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.68.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Cisco - Autor

Figura 19. Ipconfig /all PC-A – PC-B escenario 2



Fuente: Autor

Empleamos en este caso igualmente el comando IPCONFIG para verificar de una manera mas detallada la configuración de cada uno de los PC indicados, resultados de la Figura 19.

2.8 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.

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

Procedemos a verificar la conectividad de extremo a extremo de nuestra red, para esto empleamos la siguiente tabla:

Tabla 17. Verificación de Conectividad - Escenario 2

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	Dirección	10.68.8.1	exitoso
PC-A	R1, G0/0/1.20	IPv6	2001:db8:acad:a: :1	exitoso

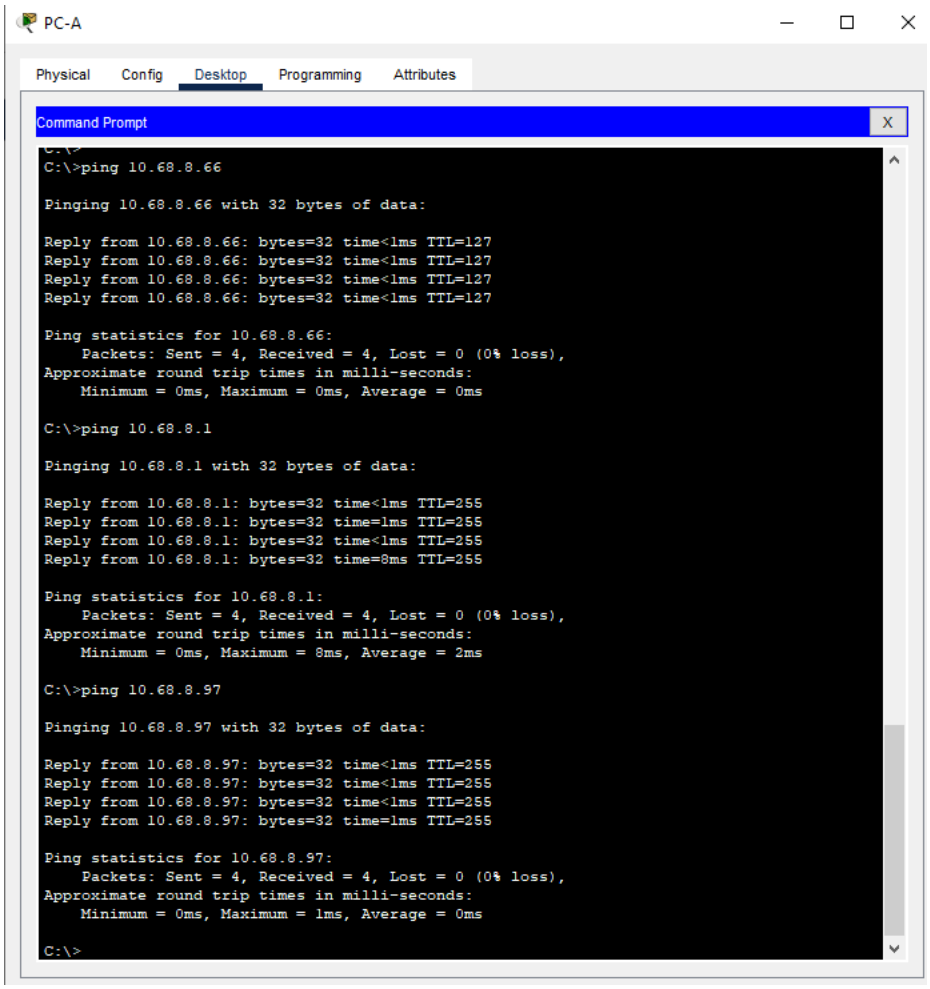
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.30	Dirección	10.68.8.65	exitoso
PC-A	R1, G0/0/1.30	IPv6	2001:db8:acad:b: :1	exitoso
PC-A	R1, G0/0/1.40	Dirección	10.68.8.97	exitoso
PC-A	R1, G0/0/1.40	IPv6	2001:db8:acad:c: :1	exitoso
PC-A	S1, VLAN 40	Dirección	10.68.8.98	exitoso
PC-A	S1, VLAN 40	IPv6	2001:db8:acad:c: :98	exitoso
PC-A	S2, VLAN 40	Dirección	10.68.8.99	exitoso
PC-A	S2, VLAN 40	IPv6	2001:db8:acad:c: :99	exitoso
PC-A	PC-B	Dirección	IP address will vary.	exitoso
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	exitoso
PC-A	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	exitoso
PC-B	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	exitoso
PC-B	R1, G0/0/1.20	Dirección	10.68.8.1	exitoso
PC-B	R1, G0/0/1.20	IPv6	2001:db8:acad:a: :1	exitoso
PC-B	R1, G0/0/1.30	Dirección	10.68.8.65	exitoso
PC-B	R1, G0/0/1.30	IPv6	2001:db8:acad:b: :1	exitoso
PC-B	R1, G0/0/1.40	Dirección	10.68.8.97	exitoso
PC-B	R1, G0/0/1.40	IPv6	2001:db8:acad:c: :1	exitoso
PC-B	S1, VLAN 40	Dirección	10.68.8.98	exitoso
PC-B	S1, VLAN 40	IPv6	2001:db8:acad:c: :98	exitoso
PC-B	S2, VLAN 40	Dirección	10.68.8.99.	Exitoso
PC-B	S2, VLAN 40	IPv6	2001:db8:acad:c: :99	Exitoso

Fuente: *Cisco* – Autor

2.9 PRUEBAS DE CONECTIVIDAD ESCENARIO 2

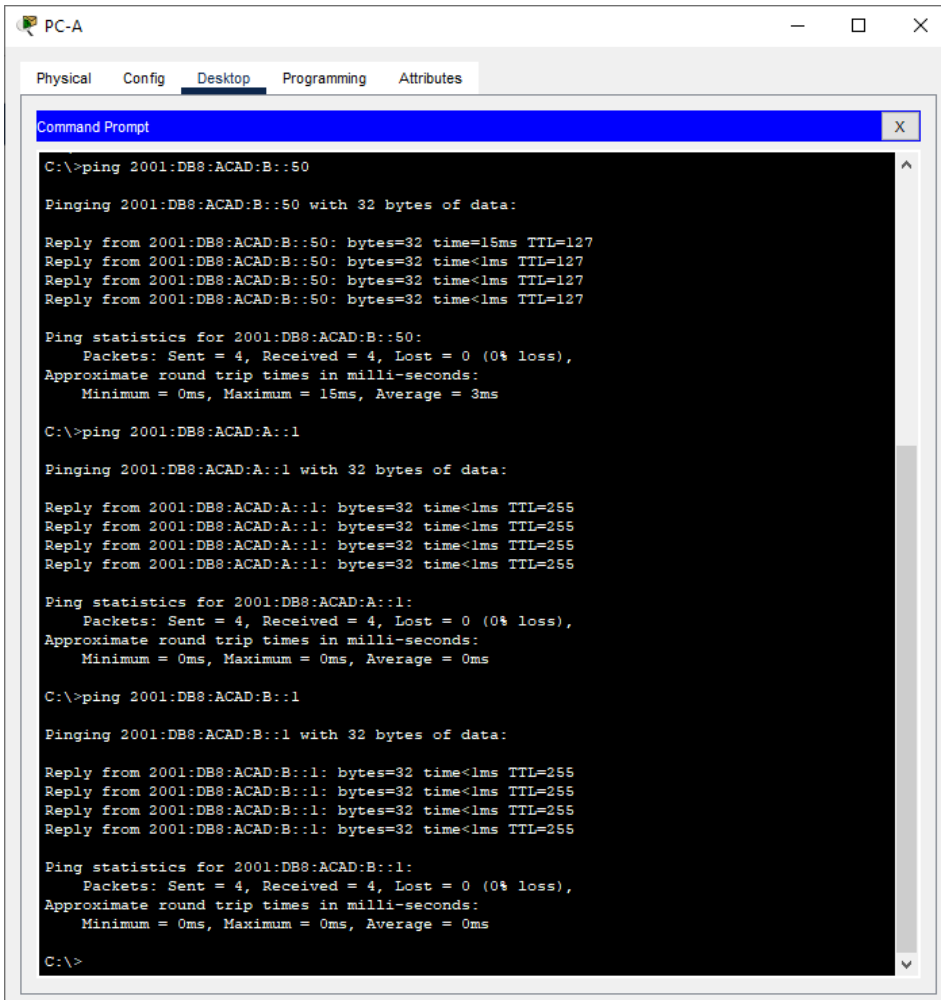
El comando PING me permito verificar si desde un punto determinado puedo llegar a otro punto de la RED y obtener respuesta del mismo, este es uno de los comandos mas utilizados con el fin de poder verificar en primera instancia la situación de mi red en genera. A continuación, realizo la verificación del estado de mi red desde diferentes equipos hacia los distintos puntos de la red, los resultados que he obtenido se muestran en las siguientes figuras:

Figura 20. PING IPV4, desde **PC-A** hacia los diferentes puntos de la red.



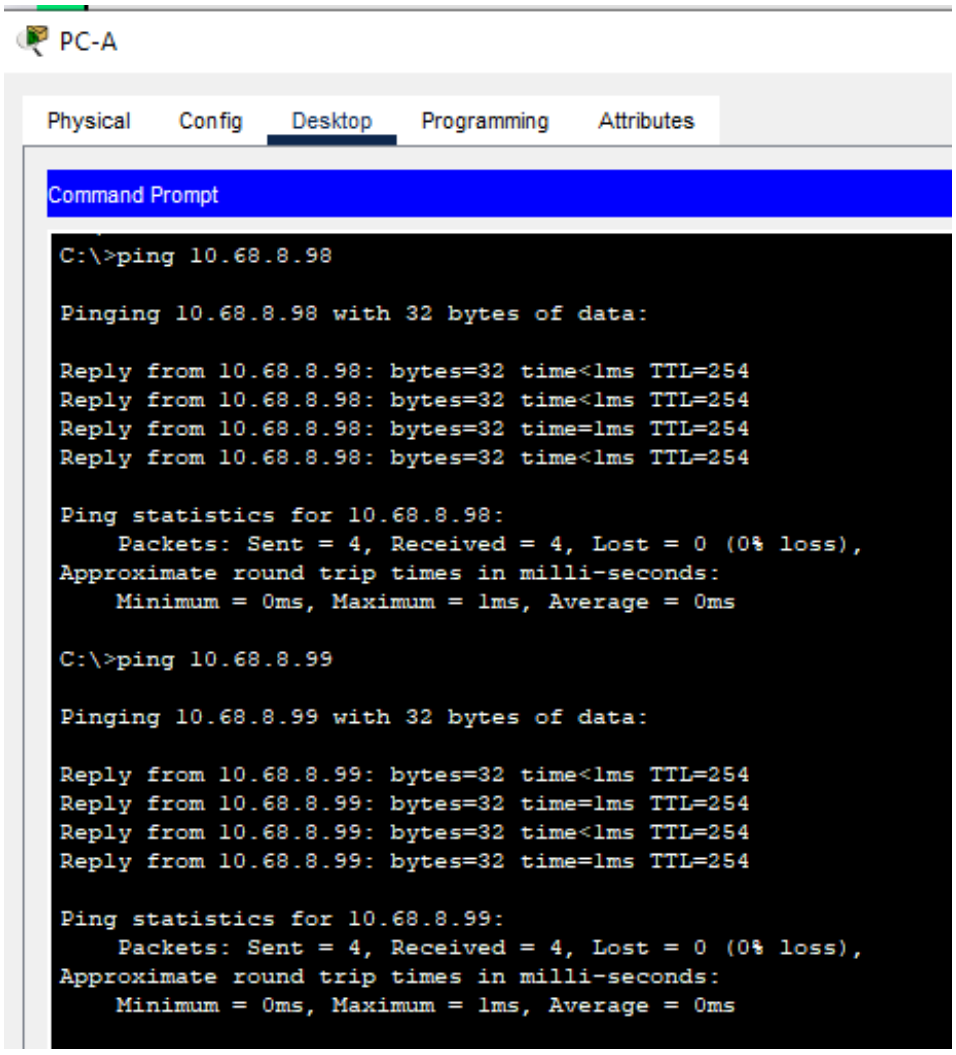
Fuente: autor.

Figura 21 - PING IPV6, desde **PC-A** hacia los diferentes puntos de la red.



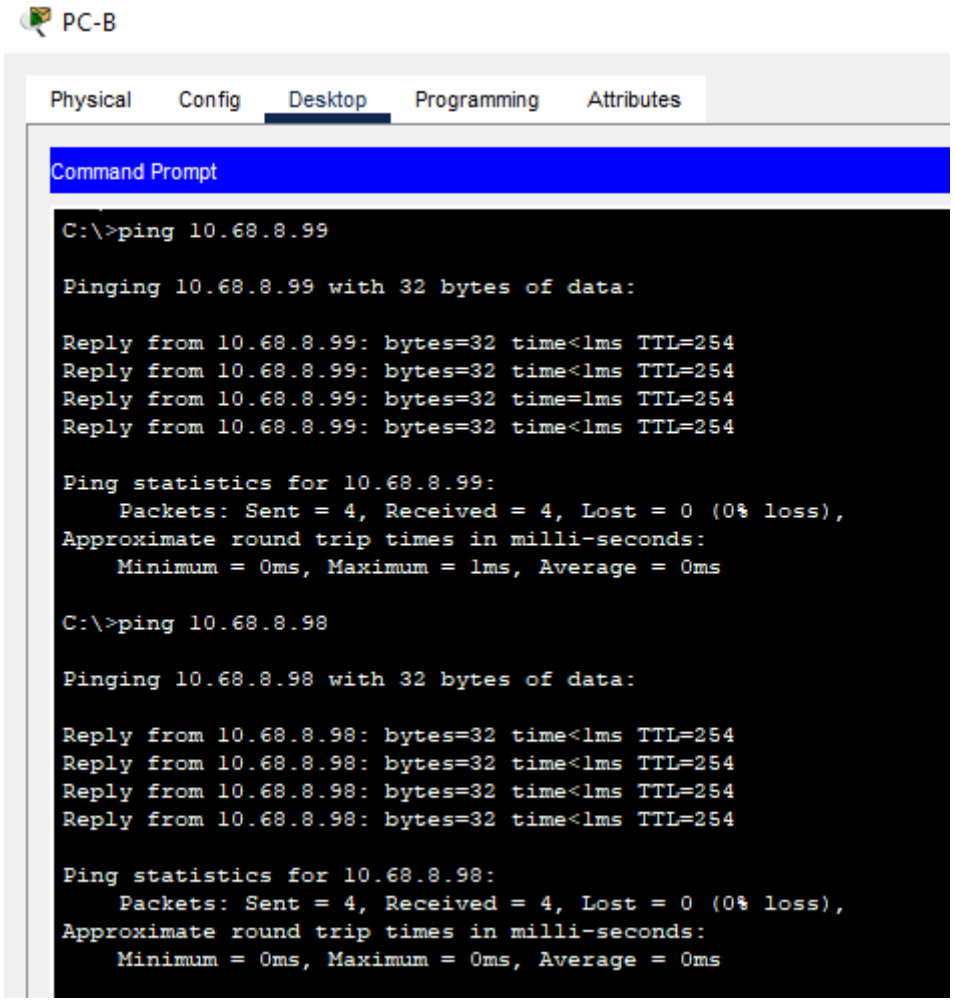
Fuente: autor.

Figura 22 - PING desde PC-A hacia la VLAN 40 de S1 y S2.



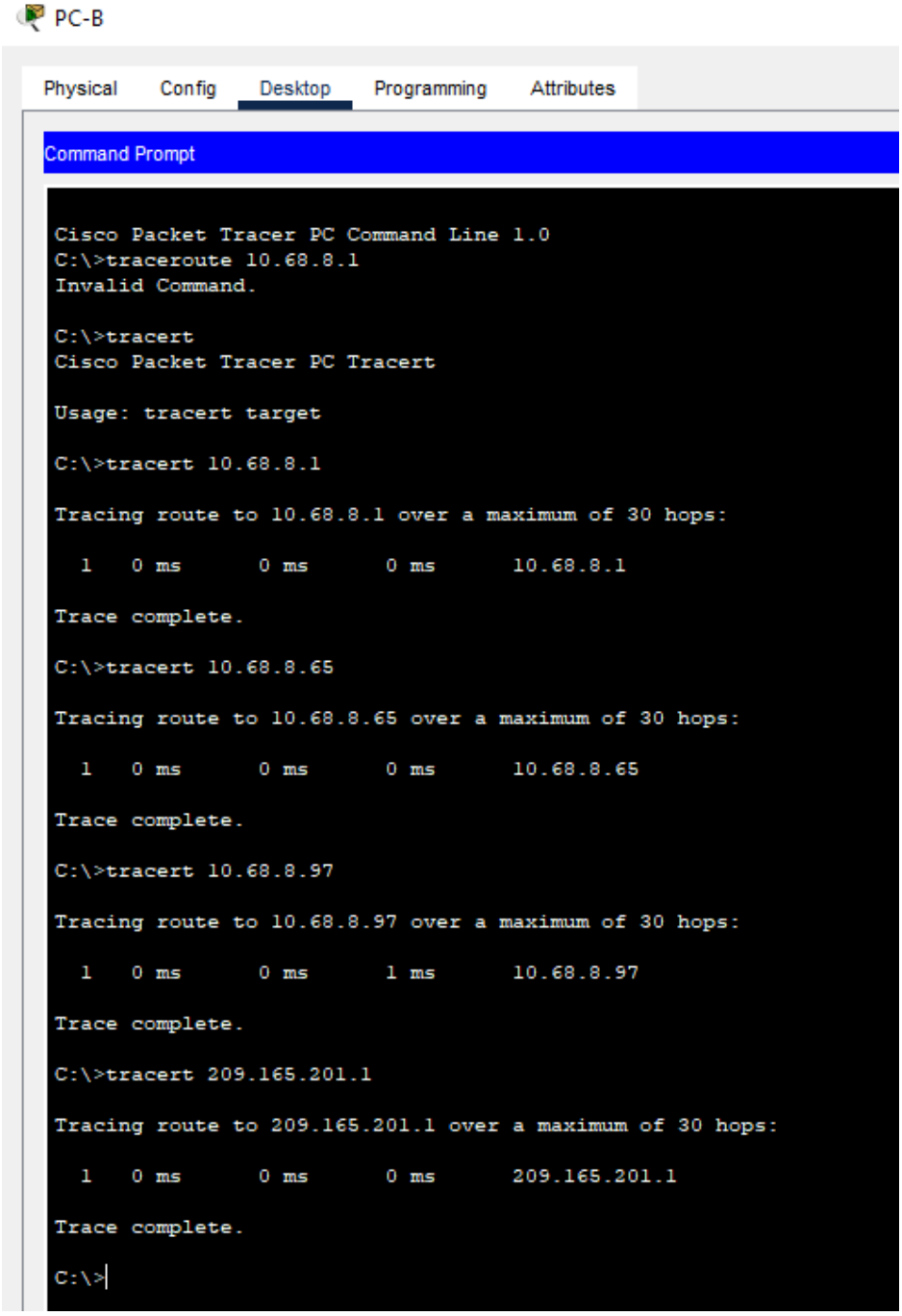
Fuente: autor.

Figura 23 - PING desde PC-B hacia la VLAN 40 de S1 y S2.



Fuente: autor.

Figura 24- TRACERT desde la PC-B hacia cada una de las subinterfaces.



Fuente: autor.

Se concluye con las pruebas realizadas anteriormente que la red es CONVERGENTE, tengo acceso hacia cada uno de los puntos de la red sin ningún inconveniente.

CONCLUSIONES

Se logró realizar la configuración de las 2 redes locales corporativas indicadas bajo la tecnología de CISCO empleando el simulador de PACKET TRACER con lo cual se puede verificar el grado de asimilación de las temáticas tratadas a lo largo del Diplomado, logrando esa satisfacción de una meta más cumplida.

Gracias al desarrollo de esta actividad se profundiza en aspectos de vital importancia para nuestro tiempo, como lo son las telecomunicaciones, aspecto que como profesionales de esta rama del saber muy seguramente aplicaremos dentro de nuestras vidas profesionales logrando el desarrollo de proyectos de cualquier envergadura.

Se realiza la configuración de cada uno de los dispositivos y tal como hemos podido comprobar mediante este proceso se comprende la importancia que radica en configurar cada uno de los aspectos básicos de los mismos, que me permiten identificar de manera sencilla y dar seguridad a cada uno de ellos.

En el caso del escenario 1 vemos que la red es pequeña, todas las LAN están conectadas directamente al mismo Router, por lo cual no se tiene la necesidad de configurar un protocolo de enrutamiento, ni crear rutas estáticas o rutas por defecto, en el caso del direccionamiento IP de los PC se hace de manera estática, para lo cual solo se debe tener en cuenta los rangos asignados a cada una de las LAN, por lo tanto finalizado el proceso, nos damos cuenta que la red es funcional luego de aplicar todos los procesos de verificación de lo hecho.

Ahora que hemos visto el ejercicio anterior nos enfocamos en el caso del Escenario 2 observamos que la red es más compleja tanto en la parte física como en la parte lógica. Iniciamos con la configuración de los protocolos de direccionamiento, a lo cual aplicamos VLSM con el fin de poder obtener varios rangos IP y de esta manera asignar los mismos a cada una de las redes locales ajustados a las necesidades reales de cada uno, de igual manera empleamos para esto tanto direcciones IPV4 como IPV6. Dentro de la red en general se configuró varias VLAN que me permitió observar la forma como podemos dividir una Red grande en varias LAN virtuales lo cual me brinda seguridad y mayor organización. En una sección de la red se configuró DHCP y observamos como de una manera automática podemos asignar direcciones IP a secciones de la red donde muy seguramente los dispositivos no permanecen habitualmente. Se agrega todo lo relacionado con la seguridad lógica de los dispositivos, esto ya que debemos recordar que la integridad de la organización depende en gran medida de este aspecto. Se culmina realizando todas las pruebas de conectividad y se verifica el correcto funcionamiento de la misma.

BIBLIOGRAFÍA.

ALBRIGHTSON, Robert. EIGRP--A fast routing protocol based on distance vectors. {En linea}. (1994). {20 noviembre 2022}. Disponible en: https://escholarship.org/content/qt9h48b8x2/qt9h48b8x2.pdf

ALEMANY, Eric David. RIP (Routing information Protocol) Análisis y simulación. {En línea}. (2018). {25 noviembre 2022}. Disponible en: https://rdu.iua.edu.ar/handle/123456789/1843

CISCO. Networking Academy. Ccna Exploration 4.0. Conceptos y protocolos de enrutamiento, Fundamentos de Networking. Cisco Systems. (2008). {20 noviembre 2022}.

CISCO. Networking Academy Ccna Exploration 4.0. Conceptos y protocolos de enrutamiento, Principios de enrutamiento. Cisco Systems. (2007). {01 noviembre 2022}.

GOITIA, María Julieta. Protocolos de enrutamiento para la capa de red en arquitecturas de redes de datos. Argentina, Universidad Nacional de Nordeste, Departamento Informática. {En línea} (2004). {23 noviembre 2022}. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/37383635/ProtocolosRed-with-cover-page-v2.PDF?Expires=1669554797&Signature=bnmMXnGCw8cLn3IeclJV~rhutlPO419GErCHPhikyNLdSFokIvGyxumJ0Bjsi7q5d7Mi7MAKGe2E~CbqH1fj1nxm0hWM7OdjXlat2P6YisHeuYzKMAqHl7tZR4txsiaVIuPIuijaeJ4UxlAoio3hhFCdbCc95~jV4OCe3fK7HR2Upvv3yos0-SNlUbyv6ZyIRK0D7UBfcxsTRqSp68-Nng9d-soAJEJzTZrw-5PUVo84po~vhKW3gHPnWnOn~ixgzuNCXcLztK8BAJzIFDAJ91S8-fzs2KEQcwcZf6VzFbLPocKCqy66UEnLlJJ5I7Ge1zj4fTIKo8U-T2IXguN~lw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

MOY, John T. OSPF: anatomy of an Internet routing protocol. Addison-Wesley Professional, {En línea}. (1998). {25 noviembre 2022}. Disponible en: https://books.google.com.co/books?hl=es&lr=&id=YXUWsqVhx60C&oi=fnd&pg=PR10&dq=ospf+routing+protocol&ots=KzBLSc3TG6&sig=KgxkYDp67mZsGBmqST9jTaD5P68#v=onepage&q=ospf%20routing%20protocol&f=false

ANEXOS

Anexo A - Enlace de descarga de simulación de escenarios.

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/hvortega_unadvirtual_edu_co/EvJlpSoOmFBHkHgjkE_XfjwB4GLsfIPTZIT2qwAOCKoorg?e=kt3c6c