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

ANA MILENA ARANDA CUASPA

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

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

ANA MILENA ARANDA CUASPA

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
PASTO
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

Firma Presidente del Jurado.

_____

Firma del Jurado

_____

Firma del Jurado

PASTO, 22 de noviembre del 2022

AGRADECIMIENTOS

En esta etapa de mi vida, punto de gran satisfacción profesional, ya que me encuentro a tan solo un paso de cumplir esta gran meta. Logro que solo ha sido posible gracias a mi institución, profesores, personas que aportaron las herramientas necesarias para mi formación, agradezco infinitamente todo ese tiempo dedicado a formarnos de una manera integral.

Agradezco a Dios por ser ese puntal y esa mano cuando más lo he necesitado, por acompañarme en cada uno de los pasos que he dado, por darme paciencia cuando la he necesitado y darme todo el conocimiento necesario para poder culminar cada una de las actividades. Mi familia pues gracias a ellos ha sido posible culminar cada una de estas etapas, por demostrarme que todo es posible con dedicación y esfuerzo, por permitirme compartir con ellos cada uno de estos logros y por ayudarme a superar los inconvenientes.

Les agradezco a mis amigos que a lo largo de mi carrera compartimos muchos momentos, por ayudarnos a superas las dificultades que solo con el apoyo incondicional de cada uno de ellos fue posible superar, gracias y comparto todo este entusiasmo con ellos pues también se encuentran finalizando sus carreras.

A todos los tutores de la Institución que me brindaron su conocimiento para formarme como profesional, como persona y como parte íntegra de una sociedad.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ADSL ASYMMETRIC DIGITAL SUBSCRIBER LINE**.** Línea Digital Asimétrica de Abonado. Sistema asimétrico de trasmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades de 1,5 y 6 Megabits por segundo en un sentido y entre 16 y 576 Kilobits en el otro[1].

DNS DOMAIN NAME SYSTEM. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1[2].

FTP. File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros más usado en Internet[3].

GATEWAY: Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red[4].

ICMP: Protocolo Internet de Control de Mensajes[5].

ROUTER: Dispositivo intermediario en las redes que se asegura de que la información no va a donde no es necesario; la labor principal de un Router es disipar y coordinar la información perteneciente a las direcciones lógicas de Red en un sistema[6].

SWITCH: es un dispositivo de red que funciona como un repartidor y sirve para segmentar una red en diferentes dominios de difusión[7].

VLSM: Las máscaras de subred de tamaño variable (variable length subnet mask, (VLSM) representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP (1987) y otras como la división en subredes (1985), el enrutamiento de Inter dominio CIDR (1993), NAT y las direcciones IP privadas[8].

---

[1] MAXWELL, Kim. Asymmetric digital subscriber line: Interim technology for the next forty years. IEEE Communications Magazine. (1996).

[2] MAESTRE, Javier. El derecho del nombre de dominio. (2001)

[3] NAGAOKA, N.; AMETANI, A. A development of a generalized frequency-domain transient program-FTP. (1988).

[4] FENG, W.C. A self-configuring RED GATEWAY. (1999)

[5] POSTEL, Jon. *Internet control message protocol*. (1981).

[6] MATURRO Gerardo; Guía para laboratorios de redes (2007)

[7] FROOM, R. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. (2015).

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

RESUMEN

El diplomado ha sido de gran utilidad para profundizar en el mundo de las telecomunicaciones, mediante el desarrollo de estos 2 ESCENARIOS que se ajustan a situaciones reales de nuestras vidas profesionales. Este trabajo ha permitido profundizar muchísimo tanto en aspectos como Dispositivos intermedios, medios de comunicación que permiten la conexión de estos dispositivos.

En todo el trabajo se ha aplicado lo relacionado con el direccionamiento aplicando VLSM tanto para direcciones IPV4 como para IPV6, de esta manera se aprecia que el direccionamiento se ajusta a las necesidades reales de cada uno de los escenarios.

Los 2 escenarios se desarrollan empleando la herramienta PACKET TRACER, la cual permite poner en práctica la configuración de cada uno de los dispositivos que hacen parte de la RED, se puede navegar por cada uno de ellos y observar las diferentes posibilidades de configuración.

En el caso del ESCENARIO 1 se realiza la configuración básica de cada uno de los dispositivos, nombre, contraseñas, dominios, direccionamiento IP y luego de todo este proceso se realiza la verificación de las etapas hechas anteriormente. Para el caso del ESCENARIO 2 se realizó el montaje de la red en PACKET TRACER se realiza la conexión de cada uno de los dispositivos según la topología entregada y se procede a realizar la configuración, inicialmente se verifica que no exista configuración previa dentro de los dispositivos, se realiza la configuración básica de cada dispositivo, las contraseñas y se procede a configurar cada una de las interfaces de los dispositivos, se crean las VLAN los enlaces TRONCALES y se configura los SERVICIO DHCP, para culminar se realizan las pruebas pertinentes de verificación de todo el proceso realizado.

Se realiza la respectiva documentación con el fin de tener un soporte escrito y bien documentado de los pasos realizados. Ya en la parte del enrutamiento se abordará el estudio de una se comandos y diferentes tipos de protocolos que nos ofrecen diferentes posibilidades dependiendo de las circunstancias en la cual se lo quiere emplear.

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

ABSTRACT

The course has been very useful to delve into the world of telecommunications, through the development of these 2 SCENARIOS that are adjusted to real situations in our professional lives. This work has allowed us to delve deeply into aspects such as Intermediate Devices, means of communication that allow the connection of these devices.

In all the work, what is related to addressing has been applied, applying VLSM for both IPV4 and IPV6 addresses, in this way it can be seen that the addressing is adjusted to the real needs of each of the scenarios.

The 2 scenarios are developed using the PACKET TRACER tool, which allows you to implement the configuration of each of the devices that are part of the NETWORK, you can navigate through each of them and observe the different configuration possibilities.

In the case of SCENARIO 1, the basic configuration of each of the devices, name, passwords, domains, IP addressing is carried out, and after all this process, the verification of the stages carried out previously is carried out. For the case of SCENARIO 2, the network was assembled in PACKET TRACER, the connection of each of the devices was made according to the topology delivered and the configuration was carried out, it was immediately verified that there is no previous configuration within the devices. , the basic configuration of each device is carried out, the passwords are carried out and each of the device interfaces is configured, the VLANs are created, the TRUNK links are configured and the DHCP SERVICE is configured, to complete the pertinent verification tests of the whole process done.

The respective documentation is carried out in order to have a written and well-documented support of the steps carried out. Already in the routing part, the study of one of the commands and different types of protocols that offer us different possibilities depending on the circumstances in which it is to be used will be addressed.

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

INTRODUCCIÓN

La tecnología en la actualidad ha ganado mucho espacio, las telecomunicaciones son parte esencial dentro de la vidas, todos quieren estar conectados en tiempo real, tener acceso a la información y disponer de ella como si estuviera en nuestras manos y que todo el proceso que esto lleva sea transparente para los usuarios, no se ve directamente todo lo que se tiene que hacer para que la información cruce de un extremo hasta nuestras manos empleando infinidad de medios y dispositivos intermedios.

Se desarrollan 2 escenarios cada uno de los cuales entrega una serie de necesidades que se debe satisfacer, gracias a la configuración de todos estos aspectos se lograra aplicar todo el conocimiento que se ha adquirido a lo largo del Diplomado. Esta configuración se realizará empleando la herramienta de simulación PACKET TRACER gracias al cual se busca profundizar en los comandos de los diferentes dispositivos intermedios.

CISCO se ha convertido en una de las organizaciones pioneras dentro de esta rama de las TELECOMUNICACIONES es por esto que como profesionales es vital conocer a profundidad todos los aspectos relacionados con este maravilloso mundo.

Espero el trabajo sea de su agrado.

1. DESARROLLO DE LA PROPUESTA PARA EL ESCENARIO 1.

1.2 Escenario:

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

1.2 Topología Escenario 1.

Figura 1. Topología Escenario 1.

Fuente: Autoría Propia.

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

Se procede a configurar la red indicada la cual consta de 3 subredes mostrada en la figura 1, procedemos a configurar el Router R1 y el Swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (60 host) y la LAN2 (20 hosts).

1.3 Construya la Red

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

1.4 Desarrolle el esquema de direccionamiento IP

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

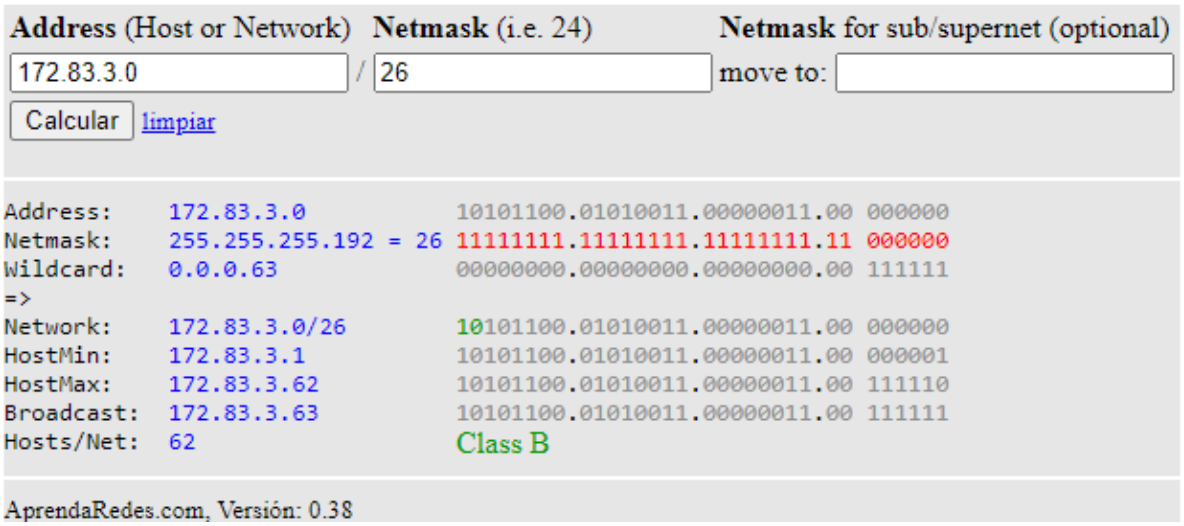
Cada estudiante tomará el direccionamiento **172.83.3.0** donde XY corresponde a

los últimos dos dígitos de su cédula.

Subneteo del rango IP:

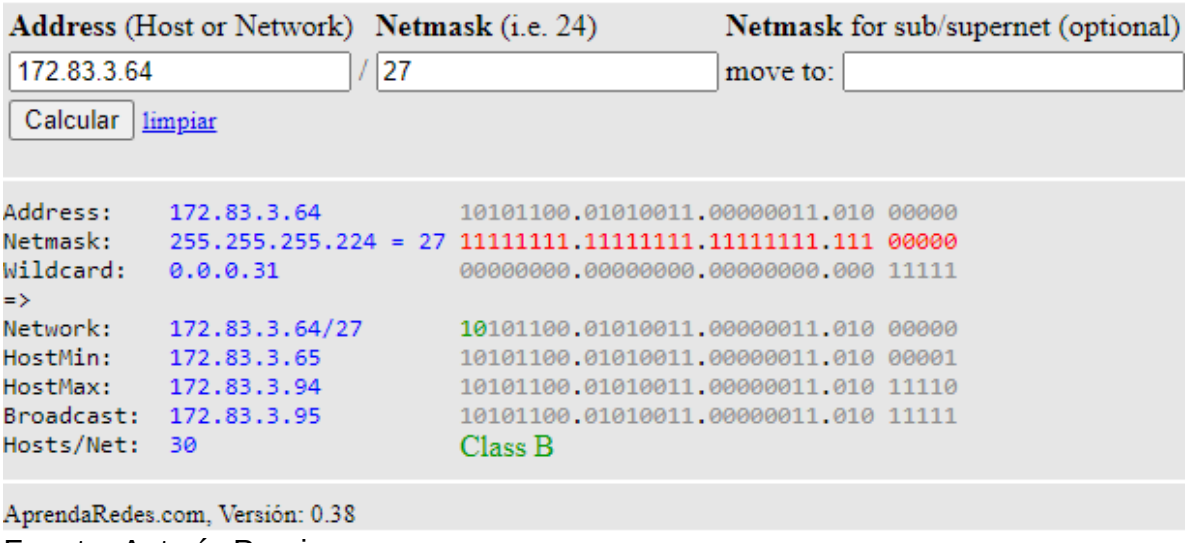
Como conocemos la topología que vamos a desarrollar y la cantidad de direcciones que cada uno de ellos nos exige para cumplir con sus necesidades podemos proceder a subnetear la dirección que se nos suministra de la siguiente manera:

Figura 3. Subneteo LAN 1.



Fuente: Autoría Propia.

Figura 4. Subneteo LAN 2.



Fuente: Autoría Propia.

La red en general está formada por 2 subredes, procedo a discriminar la información de cada una de estas LAN:

Tabla 1- Asignación de subredes.

RED	N° IP	DIR RED	MASC	/	BROADCAST	DISPONIBLES	N° HOST
LAN 1	60	172.83.3.0	255.255.255.192	26	172.83.3.63	62	60
LAN 2	20	172.83.3.64	255.255.255.224	27	172.83.3.95	30	20

Fuente: Diplomado profundización Cisco

En este punto de nuestro diseño ya conocemos los 2 rangos que vamos a emplear, por consiguiente, procedemos a asignar la dirección IP que le corresponde a cada una de las interfaces que intervienen según las indicaciones que se nos suministra:

Procedemos a realizar la asignación a cada interfaz y a realizar las primeras configuraciones a cada uno de los dispositivos.

Tabla 2. Configuración básica y asignación de direcciones IP.

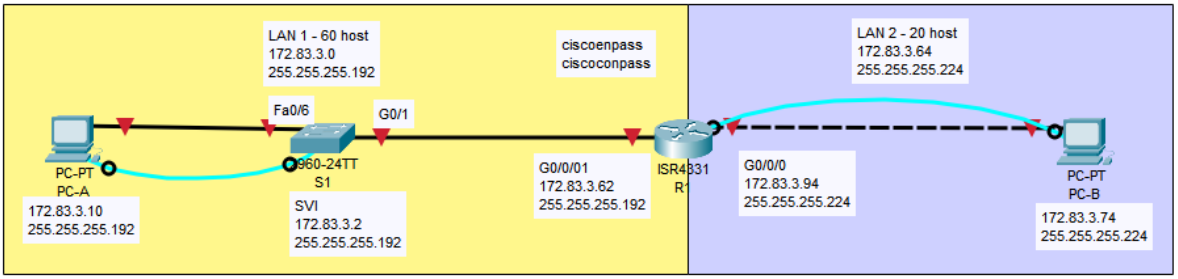
Item	**Requerimiento**
Dirección de Red	172.X.3.0 donde X corresponde a los últimos dos dígitos de su cédula. 172.83.3.0 corresponde a la dirección IP que vamos a emplear.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1 Int g0/0/1 Ip address 172.83.3.62 255.255.255.192
R1 G0/0/0	Última dirección de host de la subred LAN2 Int g0/0/0 Ip address 172.83.3.94 255.255.255.224

S1 SVI	Segunda dirección de host de la subred LAN1 Int vlan 1 Ip address 172.83.3.2 255.255.255.192
PC-A	Décima dirección de host de la subred LAN1 IP: 172.83.3.10 Mask: 255.255.255.192
PC-B	Décima dirección de host de la subred LAN2 IP: 172.83.3.74 Mask: 255.255.255.224

Fuente: Diplomado profundización Cisco

Procedemos en este punto a asignar entonces esas direcciones IP dentro del diagrama como se muestra a continuación:

Figura 5. Asignación direcciones IP interfaces.



Fuente: Autoría Propia.

1.5 Configurar los ajustes básicos del Router.

Las tareas de configuración para **R1** incluyen las siguientes:

Ahora debemos proceder a realizar la configuración tanto del S1 como del R1, recordemos que en el diagrama de la topología ya tenemos claro cuál es la dirección que le corresponde a cada una de estas interfaces, además de la configuración básica del mismo. El proceso se indica a continuación:

Tabla 3. Configuración básica R1.

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS	Procedemos a desactivas la búsqueda DNS aplicando el siguiente comando en el router R1. No ip domain lookup
Nombre del router	Agregamos el nombre al dispositivo con el fin de poderlo identificar 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	Procedemos a configurar nuestras lineas de consola empleando la contraseña: Ciscoconpass line console 0 password ciscoconpass login
Establecer la longitud mínima para las contraseñas	Establecemos una condición con el fin de que el tamaño mínimo de las contraseñas sea 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	Este mensaje aparece cada vez que ingresamos a un dispositivo, es un mensaje persuasivo. banner motd % Se prohíbe el acceso no autorizado. %
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. Config t Int g0/0/0 Ip address 172.83.3.94 255.255.255.224
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. Configure terminal Interface g0/0/01 Ip address 172.83.3.62 255.255.255.192
Generar una clave de cifrado RSA	Módulo de 1024 bits crypto key generate rsa general-keys modulus 1024

Fuente: Diplomado profundización Cisco

Realizamos la configuración básica del R1, 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 172.83.3.62 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#

R1(config-if)#int g0/0/0
R1(config-if)#ip address 172.83.3.94 255.255.255.224
R1(config-if)#no shutdown
R1(config-if)#

R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-sa.com
R1(config)#
R1(config)#do wr
```

1.6 Configurar los ajustes básicos del Router.

Continuamos ahora con nuestra tarea de configuración de **S1** incluyen lo siguiente:

Tabla 4. Configuración básica S1.

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS.	Debemos desactivar la búsqueda DNS de esta manera ahorramos recursos: No ip domain lookup
Nombre del switch	Agregamos el nombre a nuestro dispositivo S1 con el fin de poderlo identificar, por lo general en redes más grandes se emplean nombres más extensos

	para identificarlos con seguridad. 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 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	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)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento int vlan 1 description subnet A ip address 172.83.3.2 255.255.255.192
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. ip default-gateway 172.83.3.62

Fuente: Diplomado profundización 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 172.83.3.2 255.255.255.192
S1(config-if)#ip default-gateway 172.83.3.62
S1(config)#do wr
```

1.7 Configurar los ajustes básicos de los PC.

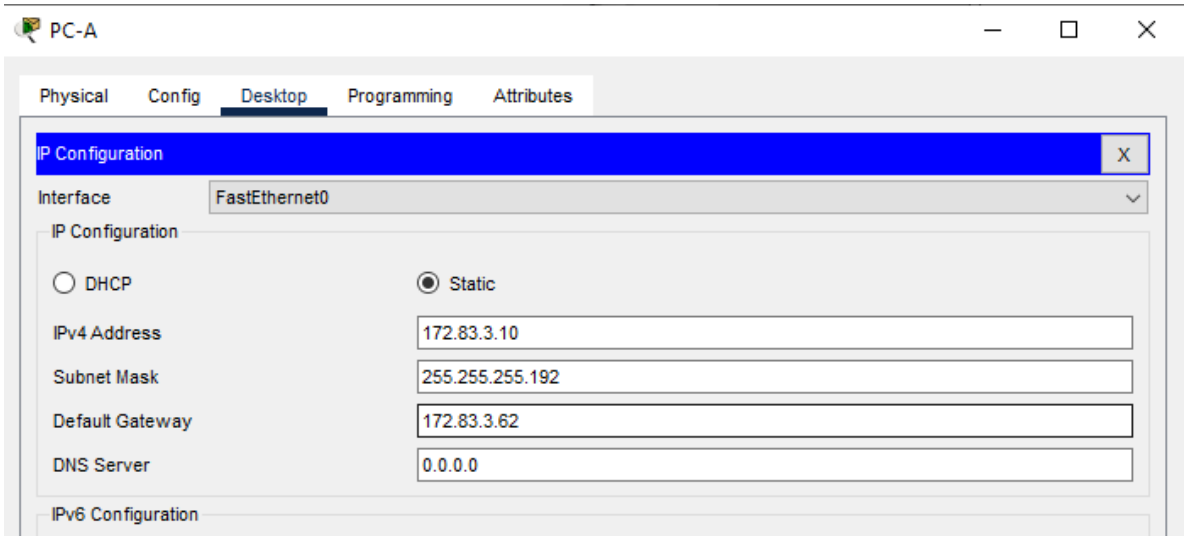
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 5. Configuración PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	
Dirección IP	172.83.3.10
Máscara de subred	255.255.255.192
Gateway predeterminado	172.83.3.62

Fuente: Diplomado profundización Cisco

Figura 6. Configuración PC-A



Fuente: Autoría Propia.

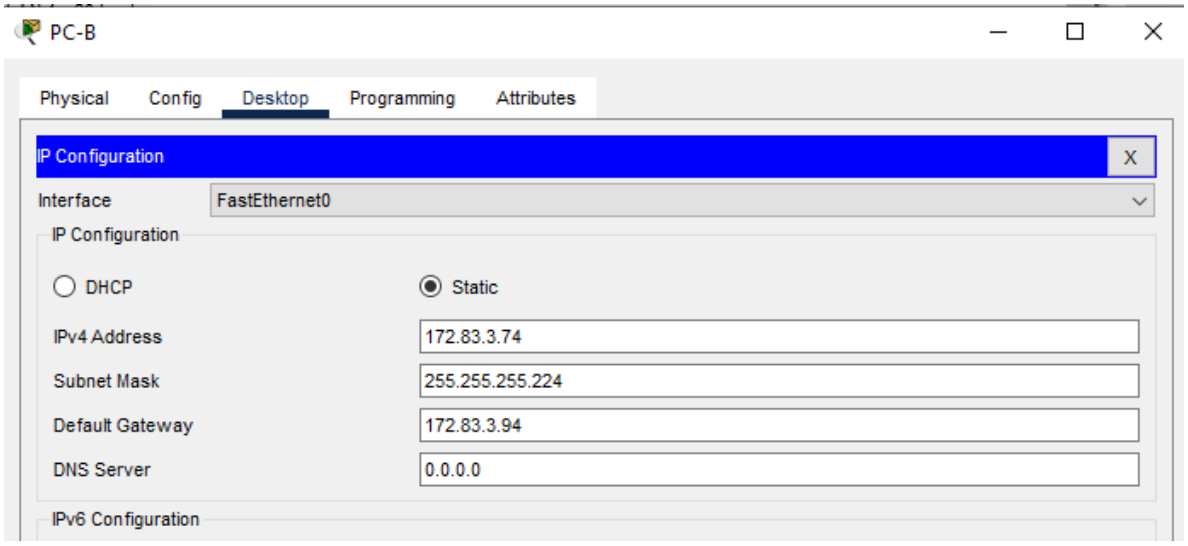
Tabla 6. Configuración PC-B

PC-B Network Configuration

Descripción	PC-B
Dirección física	
Dirección IP	172.83.3.74
Máscara de subred	255.255.255.224
Gateway predeterminado	172.83.3.94

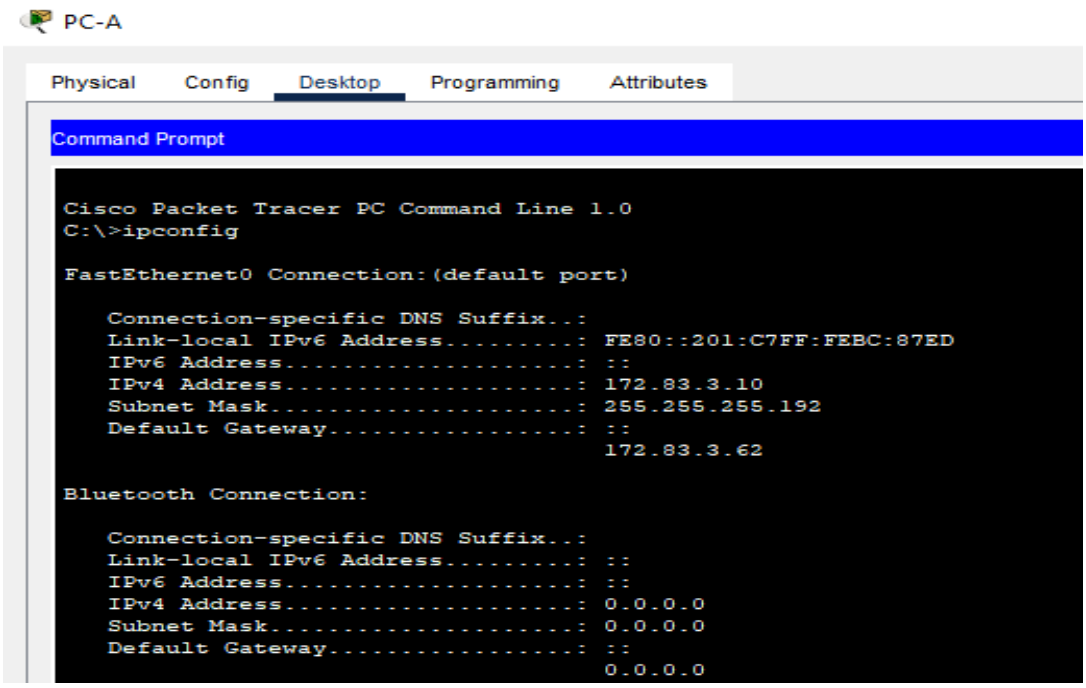
Fuente: Diplomado profundización Cisco

Figura 7. Configuración PC-B



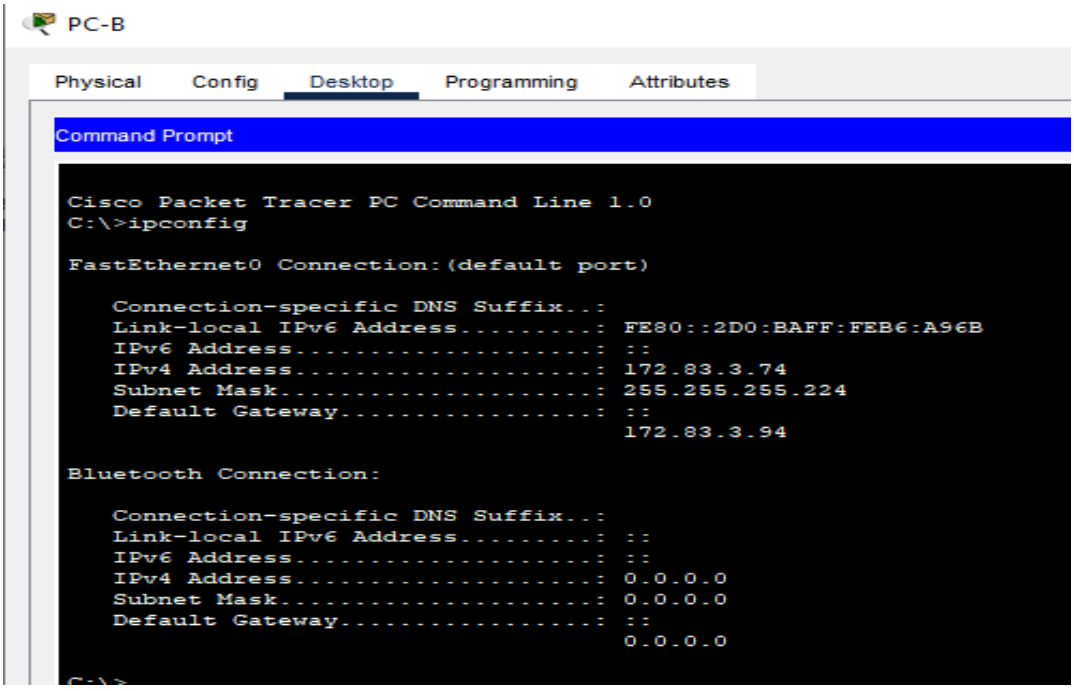
Fuente: Autoría Propia.

Figura 8. MAC PC-A



Fuente: Autoría Propia.

Figura 9. Dirección MAC - PCB

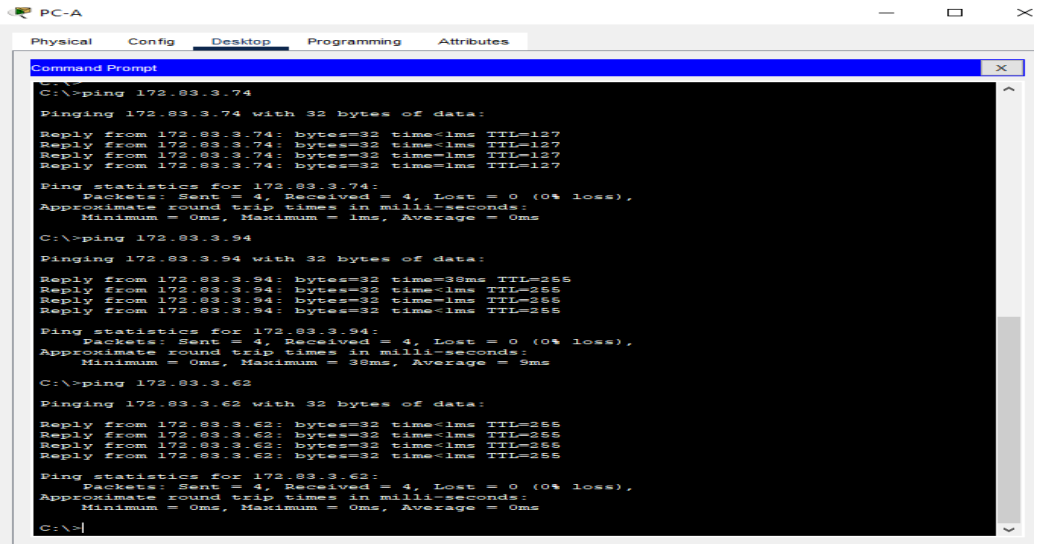


Fuente: Autoría Propia.

1.8 Pruebas de conectividad.

Desde PCA hacia los diferentes puertos de la red.

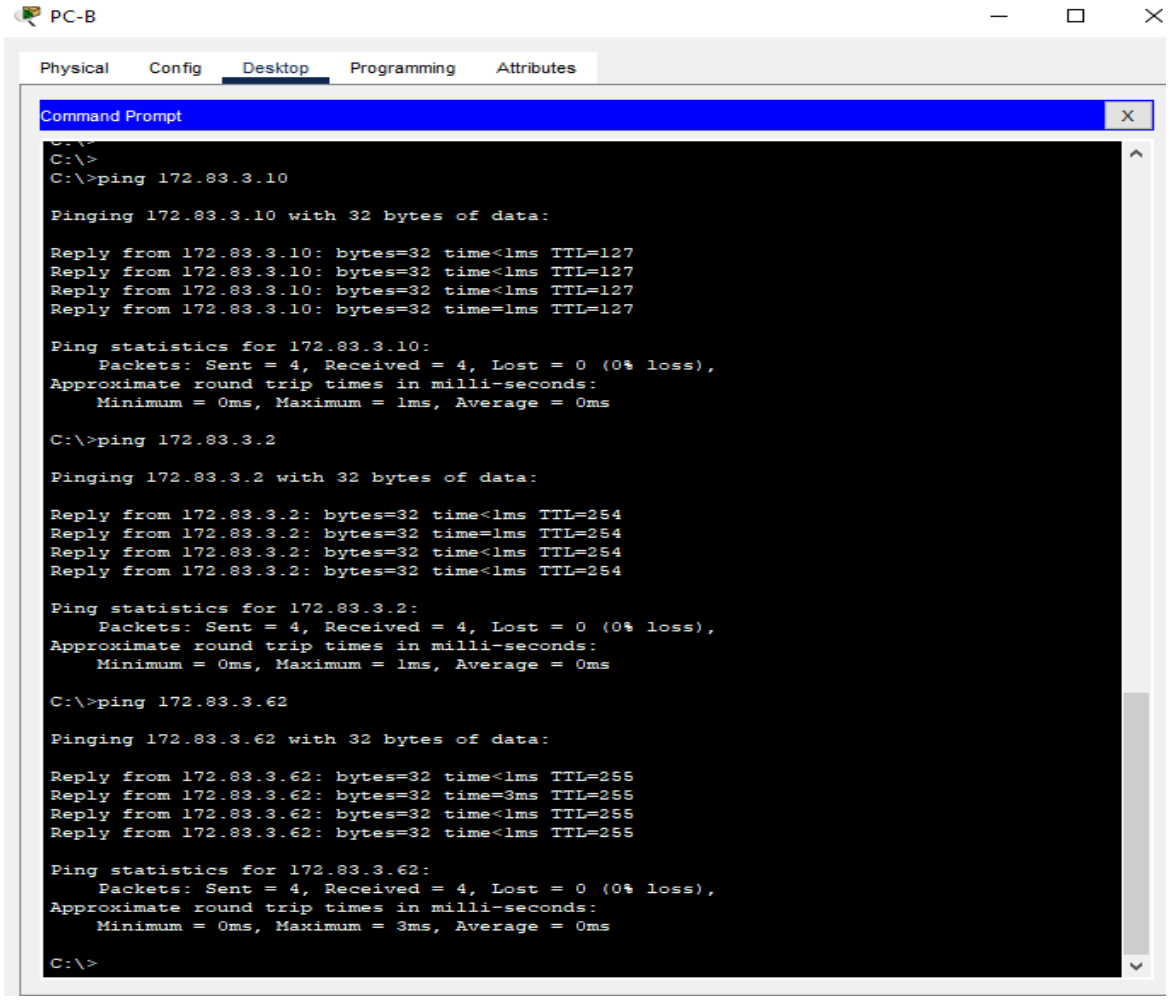
Figura 10. PING desde PC-A



Fuente: Autoría Propia.

Procedemos a realizar la verificación de lo hecho hasta el momento, para nuestro caso vamos a emplear el comando PING desde PCB hacia los diferentes puntos de la red.

Figura 11. PING desde PCB hacia los diferentes puntos de la red.



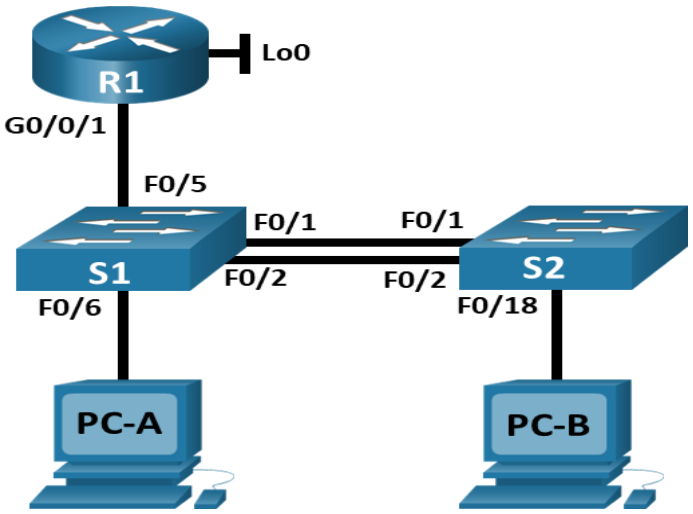
Fuente: Autoría Propia.

2. CASO DE ESTUDIO: ESCENARIO 2

Descripción de escenarios propuestos para la prueba de habilidades

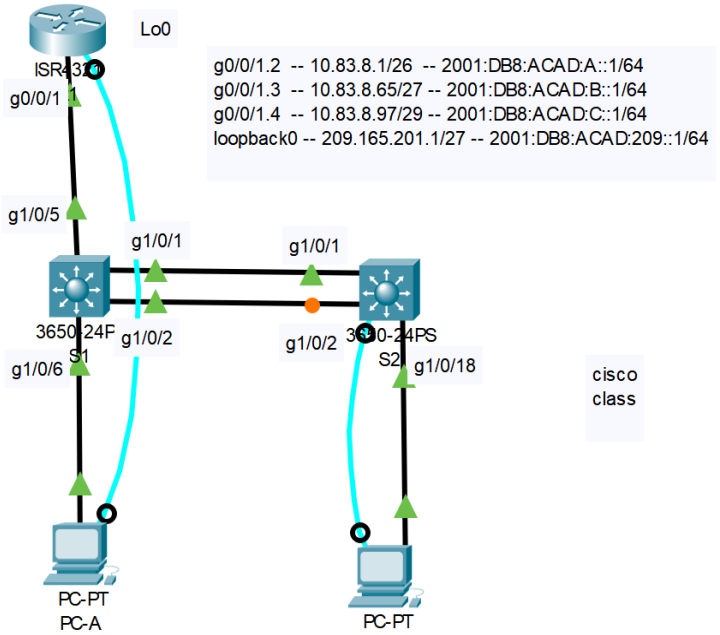
2.1 Topología Escenario 2

Figura 12. TOPOLOGIA ESCENARIO 2 – Prueba de habilidades.



Fuente: Autoría Propia.

Figura 13. TOPOLOGIA ESCENARIO 2 – Packet Tracer.



Fuente: Autoría Propia.

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

2.2 lista de Tabla de VLAN

Tabla 7. Tabla De VLAN Escenario 1.

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

Fuente: Diplomado profundización Cisco

2.3 tabla de asignación de Direcciones.

Tabla 8. Tabla de asignación de direcciones.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.83.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.83.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.83.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
S1 VLAN 4	10.83.8.98 /29	10.83.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.83.8.99 /29	10.83.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	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: Diplomado profundización Cisco

2.4 Configurar aspectos básicos de los dispositivos.

Como primer paso debemos Inicializar y volver a cargar el Router y el switch:

Debemos eliminar las configuraciones que tengan los dispositivos, de esta manera

El proceso se hace como se indica a continuación, de esta manera eliminamos cualquier tipo de configuración dentro de los dispositivos que pueda causar algún tipo de conflicto de configuración.

S1
Erase-startup-config
Delete vlan.dat
Reload
S2

Erase-startup-config

Delete vlan.dat

Reload

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

Show sdm prefer
Vemos que soporta IPV6

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

2.4.1 Configurar R1

Con el fin de poder configurar el ROUTER R1 debemos cumplir con una ser de pasos, entre ellos incluyen las siguientes:

Tabla 9. Configuración ROUTER 1.

Tarea	Especificación
Desactivar la búsqueda DNS	Evitamos que el dispositivo realice este tipo de búsquedas y consuma recursos de manera innecesaria: No ip domain-lookup
Nombre del Router	Agregamos un nombre que me permita identificar fácilmente el dispositivo Hostname R1
Nombre de dominio	Creamos un dominio con el nombre indicado, queda así: ccna-lab.com ip domain-name ccna-sa.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	Procedemos a crear las contraseñas con el fin de proteger la información, iniciamos entonces con la contraseña del modo EXEC PRIVILEGIADO: class Enable secret class
Contraseña de acceso a la consola	Se configura la contraeña de la LINEA DE CONSOLA, vital pues es un puerto de fácil acceso para cualquier persona que quiera realizar algún tipo de daño. Cisco Line console 0 Password cisco Login
Establecer la longitud mínima para las contraseñas	Por medio de este comando se busca exigir un tamaño mínimo de la contraseña, asi aseguramos que la misma tenga mayor seguridad, para nuestro caso el tamaño mínimo es de 5 caracteres. 5 caracteres Security passwords min-leng 5

Tarea	Especificación
Crear un usuario administrativo en la base de datos local.	Puede configurar nombres de usuario y contraseñas de administrador para evitar que usuarios no autorizados vuelvan a configurar el conmutador y vean la información de configuración. 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	Las líneas vty se emplean con el fin de establecer sesiones Telnet, de esta manera configuramos la misma para emplear la base de datos local y podemos así tener una sesión de manera remota. Line vty 0 15 login local
Configurar VTY solo aceptando SSH	De esta manera le indicamos al ROUTER el protocolo que será usado para conectar las líneas específicas. Transport input ssh
Cifrar las contraseñas de texto no cifrado	Las contraseñas deben estar protegidas, de esta manera que no aparezcan como archivo plano sino cifradas. Service password-encryption

Tarea	Especificación
Configure un MOTD Banner	Este mensaje es simplemente algo persuasivo, que indica la gravedad de un acceso no autorizado. banner motd & Dispositivo: ROUTER R1 Trabajo presentado por: ANA MILENA ARANDA Código: 27,090,383 Programa: INGENIERIA DE SISTEMAS Grupo: 203092_14 &
Habilitar el routing IPv6	Este comando lo que hace es habilitar el routing IPV6 en el ROUTER. Ipv6 unicast-routing

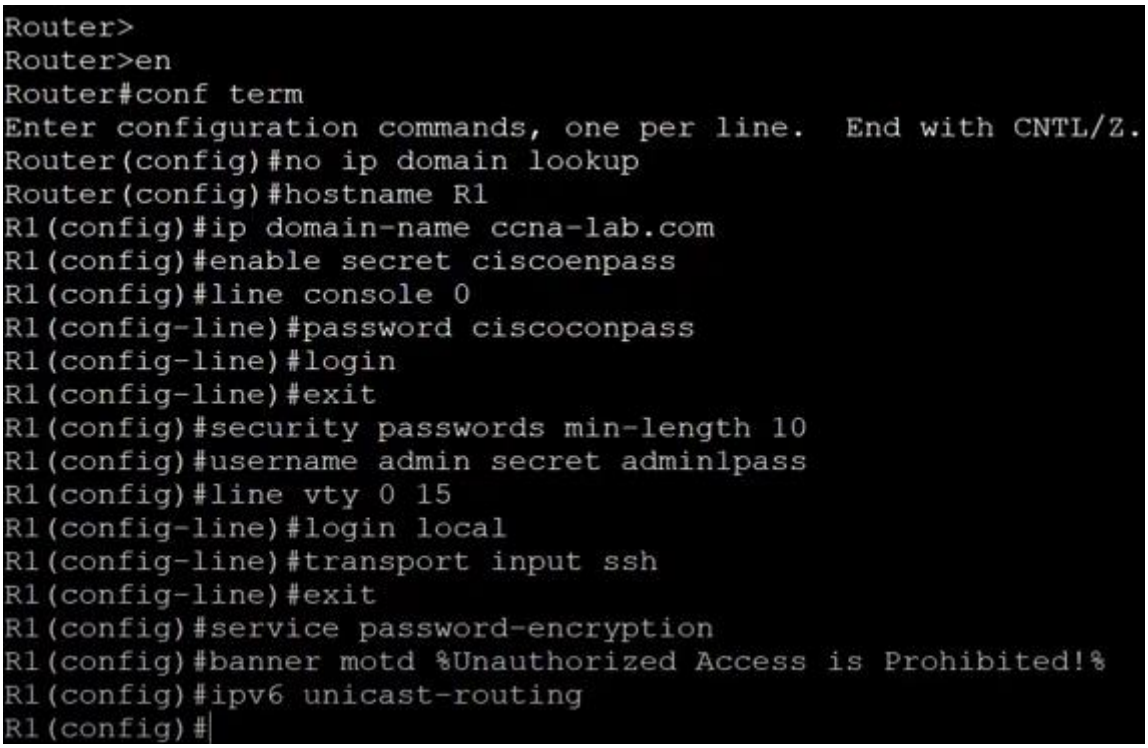
Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	Como primera parte dentro del ROUTER procedemos a configurar sus interfaces y subinterfaces, agregando una pequeña descripción de cada una de ellas que me permita identificar lo que esta conectados a cada una de ellas. Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80: :1** Activar la interfaz. Int g0/0/1.20 Encapsulation dot1q 20 Description DOCENTES Ip addres 10.83.8.1 255.255.255.192 Ipv6 addres 2001:db8:acad:a:1/64 Ipv6 addres fe80::1 link local Int g0/0/1 No shutdown Int g0/0/1.30 Encapsulation dot1q 30 Description ESTUDIANTES Ip addres 10.83.8.65 255.255.255.224 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 10.83.8.97 255.255.255.224 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 10.83.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local Ya temenos configuradas las subinterfaces, pero para finalizar debemos activar la INTERFACE. Int g0/0/1 No shutdown

Tarea	Especificación
Configure el Loopback0 interface	Ahora configuramos la interface LOOPBACK0, agregando la información indicada, esta interface simula la conexión WAN o en su defecto una salida hacia INTERNET. 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 INTERNET
Generar una clave de cifrado RSA	Crypto key generate rsa permite generar una llave RSA3 en el modo de configuración global. Módulo de 1024 bits Crypto key generate rsa modulus 1024

Fuente: Diplomado profundización Cisco

A continuación, indico el proceso de configuración básica del R1

Figura 14. Configuración del R1.



Fuente: Autoría Propia.

Con el fin de poder realizar la configuración adecuada de cada una de las subinterfaces, se indica la siguiente tabla con las direcciones IPV4 como IPV6 de cada una de ellas:

Tabla 10. Configuración interfaces router 1.

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.83.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.33	10.83.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.83.8.97 /29	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.4	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

Fuente: Diplomado profundización Cisco

2.4.2 Configure S1 y S2.

Ya dentro de este nuevo paso procedemos a realizar la configuración de los SWITCHES Las tareas de configuración incluyen lo siguiente:

Tabla 11. Configuración SWITCH 1.

Tarea	Especificación
Desactivar la búsqueda DNS.	Evitamos que el dispositivo realice este tipo de búsquedas y consuma recursos de manera innecesaria: No ip domain lookup
Nombre del switch	Agregamos un nombre que me permita identificar fácilmente el dispositivo **S1 o S2, según proceda** Hostname S1 Hostname S2

Tarea	Especificación
Nombre de dominio	Creamos un dominio con el nombre indicado, queda así: **ccna-sa.com** ip domain name **ccna-sa.com**
Contraseña cifrada para el modo EXEC privilegiado	Procedemos a crear las contraseñas con el fin de proteger la información, iniciamos entonces con la contraseña del modo EXEC PRIVILEGIADO: **class** Enable secret class
Contraseña de acceso a la consola	Se configura la contraseña de la LINEA DE CONSOLA, vital pues es un puerto de fácil acceso para cualquier persona que quiera realizar algún tipo de daño. **cisco** Line console 0 Password cisco Login

Tarea	Especificación
Crear un usuario administrativo en la base de datos local	Puede configurar nombres de usuario y contraseñas de administrador para evitar que usuarios no autorizados vuelvan a configurar el conmutador y vean la información de configuración. 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.	Las líneas vty se emplean con el fin de establecer sesiones Telnet, de esta manera configuramos la misma para emplear la base de datos local y podemos así tener una sesión de manera remota. Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	De esta manera le indicamos al ROUTER el protocolo que será usado para conectar las líneas específicas. Transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	Las contraseñas deben estar protegidas, de esta manera que no aparezcan como archivo plano sino cifradas. Service password-encryption
Configurar un MOTD Banner	Este mensaje es simplemente algo persuasivo, que indica la gravedad de un acceso no autorizado. banner motd & Dispositivo: ROUTER R1 Trabajo presentado por: ANA MILENA ARANDA Código: 27,090,383 Programa: INGENIERIA DE SISTEMAS Grupo: 203092_14 &
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa mosulus 10242

Tarea	Especificación
Configurar la interfaz de administración (SVI)	Se procede a crear y configurar la interface virtual. 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 10.83.8.98 255.255.255.248 Ipv6 address 2001:db8:acad:c::98/64 Ipv6 address fe80::98 link-local Description ADMINISTRACIÓN No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.83.8.97 para IPv4 la cual es la dirección de la (SVI) Ip Default-gateway 10.83.8.97

Fuente: Diplomado profundización Cisco

2.4.3 Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 12. Configuración SWITCH 2.

Tarea	Especificación
Desactivar la búsqueda DNS.	Evitamos que el dispositivo realice este tipo de búsquedas y consuma recursos de manera innecesaria: No ip domain lookup
Nombre del switch	Agregamos un nombre que me permita identificar fácilmente el dispositivo Hostname S2
Nombre de dominio	Creamos un dominio con el nombre indicado, queda así: ccna-sa.com ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Procedemos a crear las contraseñas con el fin de proteger la información, iniciamos entonces con la contraseña del modo EXEC PRIVILEGIADO: Enable secret class

Tarea	Especificación
Contraseña de acceso a la consola	Se configura la contraseña de la LINEA DE CONSOLA, vital pues es un puerto de fácil acceso para cualquier persona que quiera realizar algún tipo de daño. Line console 0 Password cisco Login
Crear un usuario administrativo en la base de datos local	Puede configurar nombres de usuario y contraseñas de administrador para evitar que usuarios no autorizados vuelvan a configurar el conmutador y vean la información de configuración. 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	Las líneas vty se emplean con el fin de establecer sesiones Telnet, de esta manera configuramos la misma para emplear la base de datos local y podemos así tener una sesión de manera remota. Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	De esta manera le indicamos al ROUTER el protocolo que será usado para conectar las líneas específicas. Transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	Las contraseñas deben estar protegidas, de esta manera que no aparezcan como archivo plano sino cifradas. Service password-encryption
Configurar un MOTD Banner	Este mensaje es simplemente algo persuasivo, que indica la gravedad de un acceso no autorizado. banner motd & Dispositivo: ROUTER R1 Trabajo presentado por: ANA MILENA ARANDA Código: 27,090,383 Programa: INGENIERIA DE SISTEMAS Grupo: 203092_14 &
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa 1024

Tarea	Especificación
Configurar la interfaz de administración (SVI)	Se procede a crear y configurar la interface virtual. 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 4 Ip address 10.83.8.99 255.255.255.248 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 10.83.8.97 para IPv4 la cual es la dirección de la (SVI) Ip Default-gateway 10.83.8.97

Fuente: Diplomado profundización Cisco

2.5 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

2.5.1 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 13. Configuración SWITCH 1 - (VLAN, Trunking, EtherChannel).

Tarea	Especificación
Crear VLAN	Iniciamos con la configuración de las VLAN en S1, estas quedarían como muestro a continuación: Vlan 20 Name Docentes Vlan 30 Name Estiudiantes Vlan 40 Name Invitados Vlan 50 Name Usuarios Vlan 56 Name native

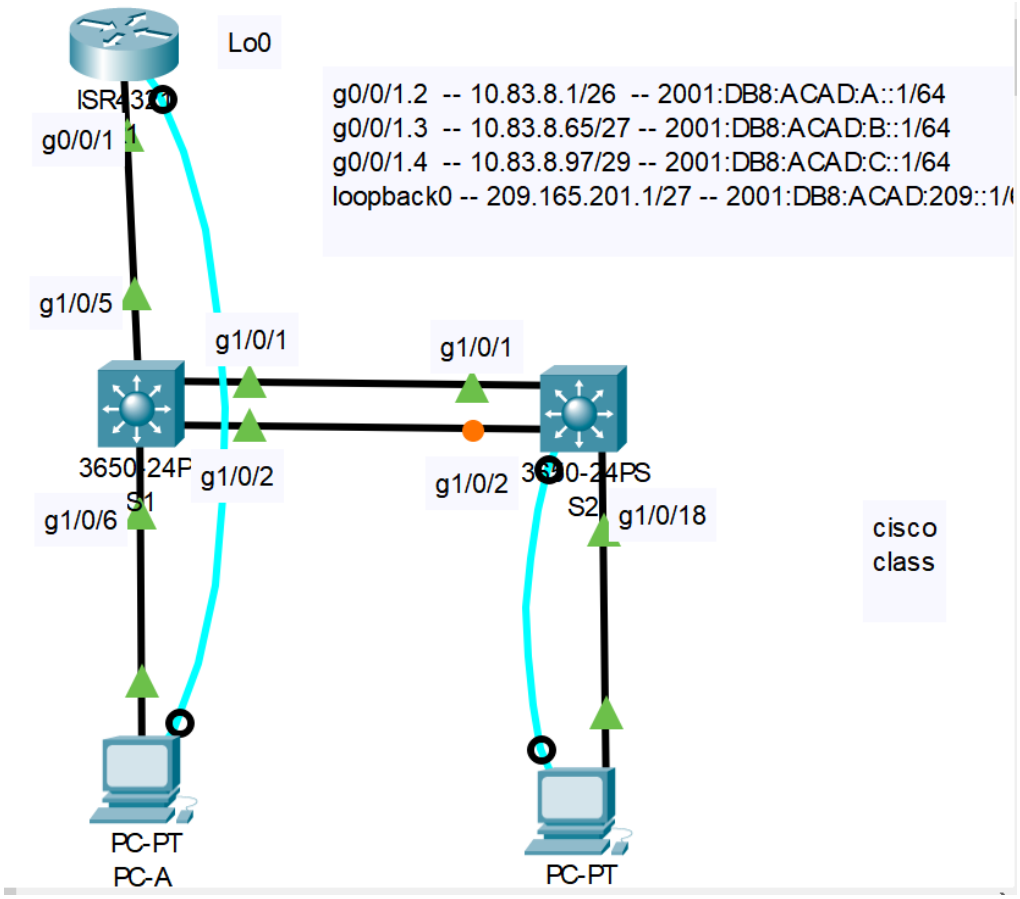
Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Procedemos a configurar las interfaces del SWITCH como troncales ya que me permiten el paso de los paquetes de diferentes VLAN. Interface G1/0/5 Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 56 Interface range G1/0/1-2 Shutdown 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 de host para VLAN 20	A la interface g1/0/6 queda conectado los dispositivos agregados a la VLAN 20, por consiguiente, luego de crear la VLAN debemos asignar los puertos a la misma: Interface g1/0/6 Interface g1/0/6 Switchport mode access Switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	Procedemos a configurar la seguridad de la interface, indicando que solo permita 3 direcciones MAC en esta: Permitir 4 direcciones MAC Switchport port-security máximum 4

Tarea	Especificación
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar. Este proceso se hace por seguridad. Int range g1/0/3-4 Switchport mode Access Switchport Access vlan 50 Description no esta en uso Shutdown Int range g1/0/7-24 Switchport mode Access Switchport Access vlan 50 Description no esta en uso Shutdown Int range g1/1/1-4 Switchport mode Access Switchport Access vlan 50 Description no esta en uso Shutdown

Fuente: Diplomado profundización Cisco

Figura 15. Configuración del S1.



Fuente: Autoría Propia.

2.5.2 Configure el S2.

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

Tabla 14. configuración SWITCH 2 - (VLAN, Trunking, EtherChannel).

Tarea	Especificación
Crear VLAN	Iniciamos con la configuración de las VLAN en S1, estas quedarían como muestro a continuación: Vlan 20 Name Docentes Vlan 30 Name Estiudiantes Vlan 40 Name Invitados Vlan 50 Name Usuarios Vlan 56 Name native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Procedemos a configurar las interfaces del SWITCH como troncales ya que me permiten el paso de los paquetes de diferentes VLAN. Interfaces range G1/0/1-2 No shutdown 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	A la interface g1/0/18 queda conectado los dispositivos agregados a la VLAN 30, por consiguiente, luego de crear la VLAN debemos asignar los puertos a la misma: Int g0/1/18 Switchport mode Access Switchport Access vlan 30
Configure port-security en los access ports	Procedemos a configurar la seguridad de la interface, indicando que solo permita 3 direcciones MAC en esta: Permite 3 MAC addresses switchport port-security switchport port-security maximum 3

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar. Este proceso se hace por seguridad. Int range g1/0/3-17 Switchport mode Access Switchport Access vlan 50 Description no esta en uso Shutdown Int range g1/0/19-24 Switchport mode Access Switchport Access vlan 50 Description no esta en uso Shutdown Int range g1/1/1-4 Switchport mode Access Switchport Access vlan 50 Description no está en uso Shutdown

Fuente: Diplomado profundización Cisco

2.6 Configurar soporte de host

2.6.1 Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configuración ROUTER 1 - loopback 0 - DHCP.

Tarea	Especificación
Configure Default Routing	En esta sección lo que se hace es crear rutas predeterminadas que me permitan enviar los paquetes hacia la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 Ipv6 route ::/0 loopback 0

Tarea	Especificación
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 10.83.8.0 /26 El rango de esta subred quedaría: 10.83.8.1 10.83.8.62 Recordemos que se deben restringir las primeras direcciones IP, ya que solo debemos trabajar con las ultimas 10 direcciones utilizables. 10.83.8.1 - 10.83.8.52 estas son las que debemos restringir y solo trabajamos con las 10 que sobran. Debemos entonces crear el POOL desde: 10.83.8.52 - 10.83.8.62 Ip dhcp excluded-address 10.83.8.1 10.83.8.52 Ip dhcp POOL VLAN20-DOCENTES Network 10.83.8.0 255.255.255.192 Default-route 10.83.8.1 Domain-name ccna-sa.net

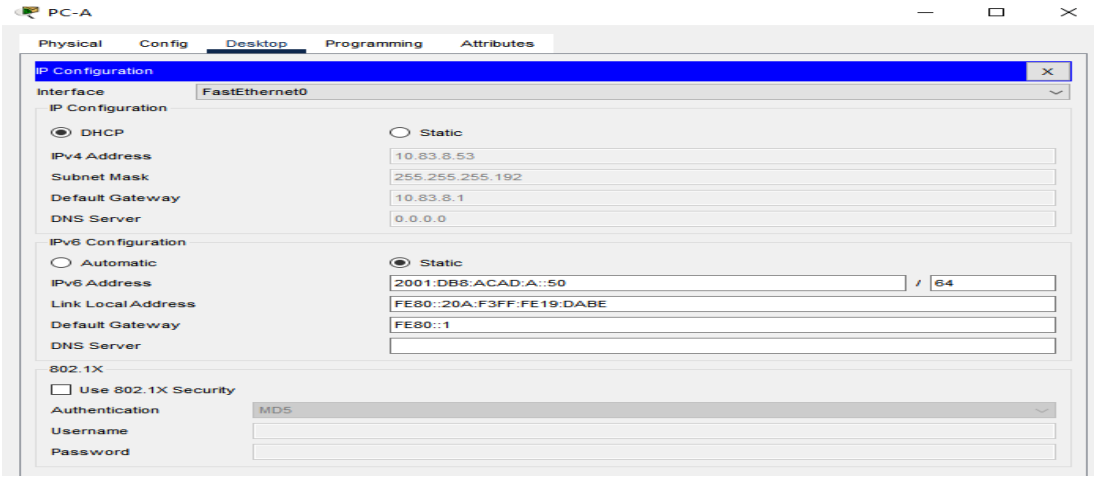
Tarea	Especificación
Configurar DHCP IPv4 para VLAN 30	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada 10.83.8.64 /27 El rango de esta subred quedaría: 10.83.8.65 10.83.8.94 Recordemos que se deben restringir las primeras direcciones IP, ya que solo debemos trabajar con las ultimas 10 direcciones utilizables. 10.83.8.65 - 10.83.8.84 este rango es el que se debe restringir, de esa manera nos quedan las 10 ultimas para poder trabajar. Debemos entonces crear el POOL desde: 10.83.8.85 - 10.83.8.94 Ip dhcp excluded-address 10.83.8.65 10.83.8.84 Ip dhcp POOL VLAN30-ESTUDIANTES Network 10.83.8.64 255.255.255.224 Default-route 10.83.8.65 Domain-name ccna-sb.net

Fuente: Diplomado profundización Cisco

2.6.2 Configurar los servidores

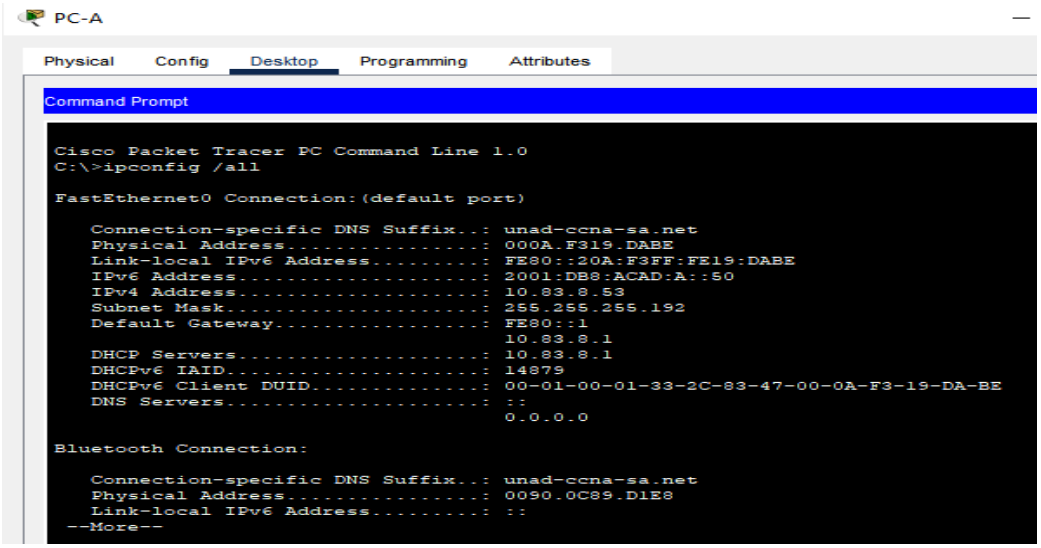
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

Figura 16. Verificación de DHCP en las PC-A.



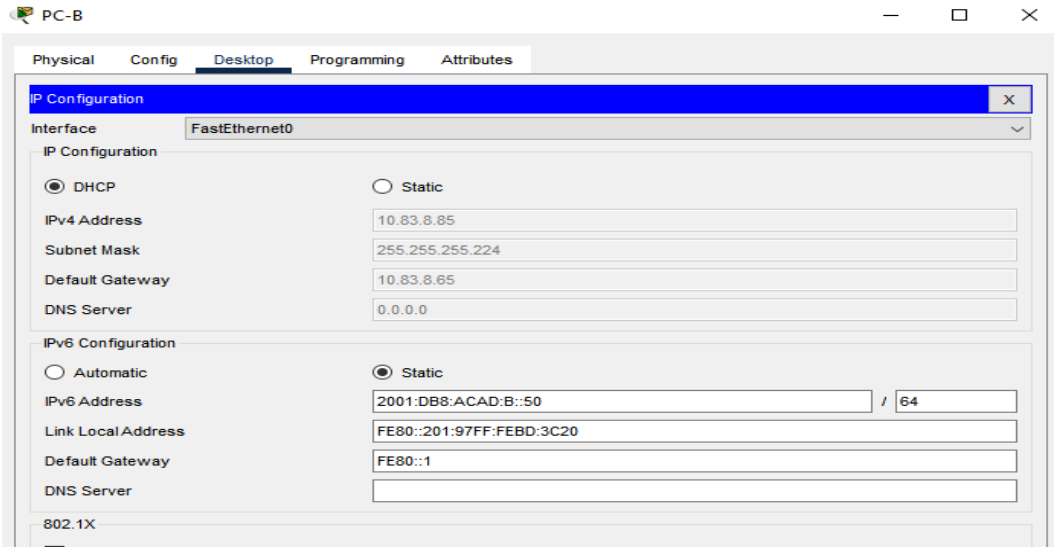
Fuente: Autoría Propia.

Figura 17. IPCONIG / ALL PC-A.



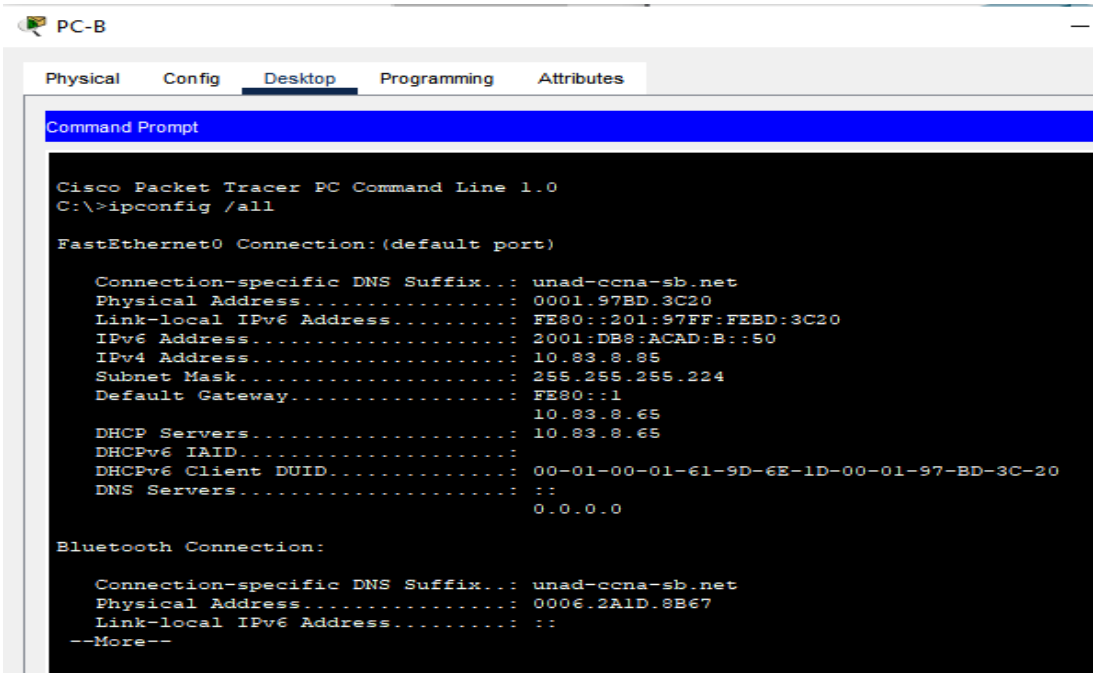
Fuente: Autoría Propia.

Figura 18. Verificación de DHCP en las PC-B.



Fuente: Autoría Propia.

Figura 19. Ipconig / all PC-B.



Fuente: Autoría Propia.

Tabla 16. Configuración DHCP PC-A – PC-B

PC-A Network Configuration	
Descripción	PC-A
Dirección física	000A.F319.DABE
Dirección IP	10.83.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.83.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Diplomado profundización Cisco

Tabla 17. Configuración DHCP PC-A – PC-B

Configuración de red de PC-B	
Descripción	PC-C
Dirección física	0001.97BD.3C20
Dirección IP	10.83.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.83.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Diplomado profundización Cisco

2.7 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.

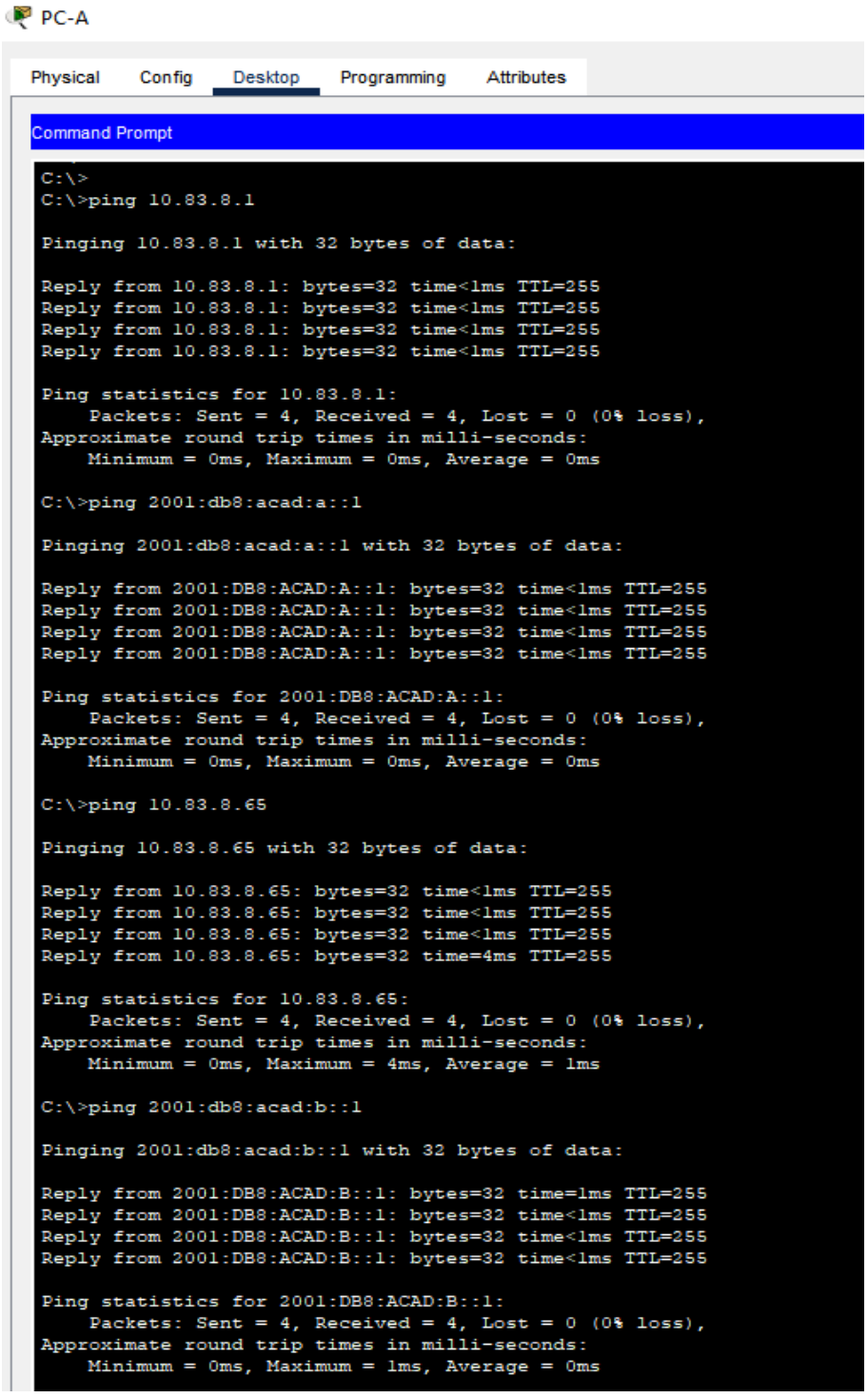
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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

Tabla 18. Pruebas de conectividad.

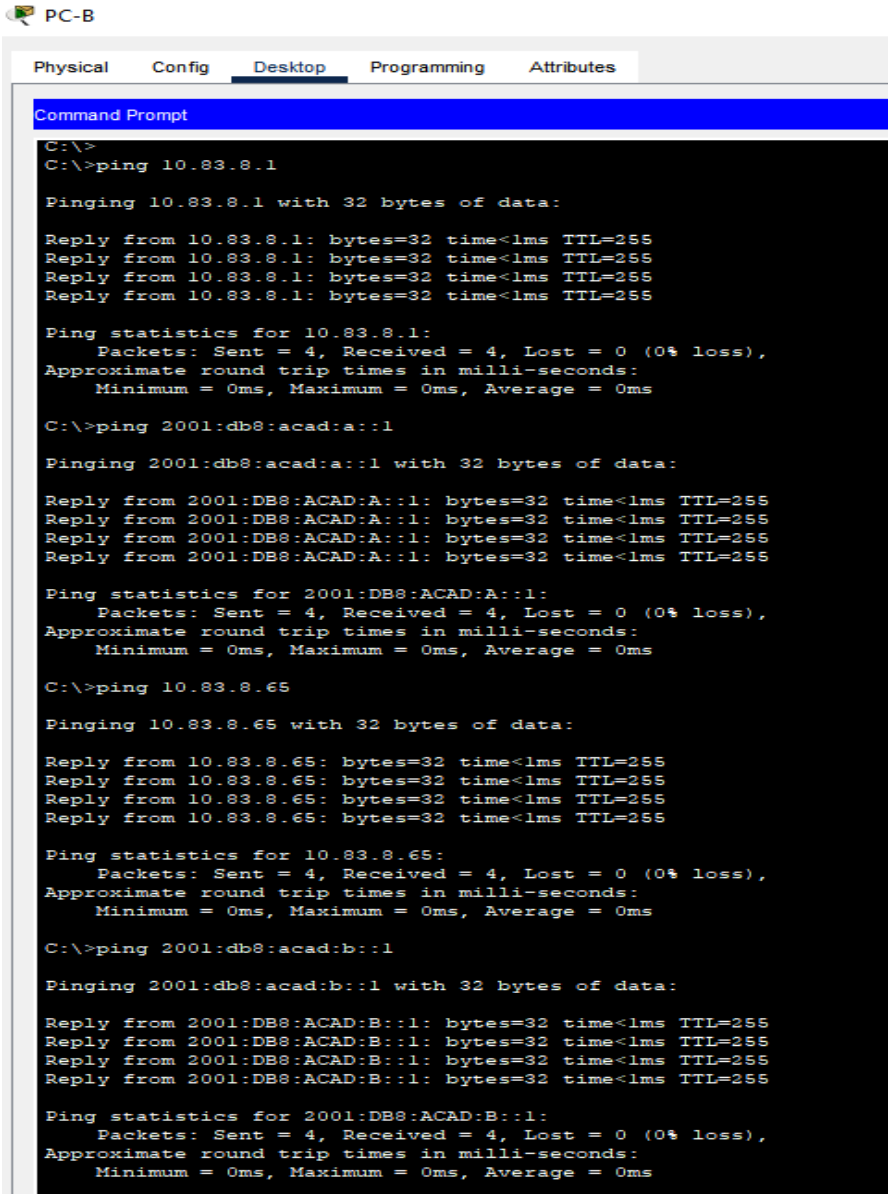
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	Dirección	10.83.8.1	exitoso
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	exitoso
PC-A	R1, G0/0/1.30	Dirección	10.83.8.65	exitoso
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	exitoso
PC-A	R1, G0/0/1.40	Dirección	10.83.8.97	exitoso
PC-A	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	exitoso
PC-A	S1, VLAN 4	Dirección	10.83.8.98	exitoso
PC-A	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	exitoso
PC-A	S2, VLAN 4	Dirección	10.83.8.99.	exitoso
PC-A	S2, VLAN 4	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	10.83.8.1	exitoso
PC-B	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	exitoso
PC-B	R1, G0/0/1.30	Dirección	10.83.8.65	exitoso
PC-B	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	exitoso
PC-B	R1, G0/0/1.40	Dirección	10.83.8.97	exitoso
PC-B	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	exitoso
PC-B	S1, VLAN 4	Dirección	10.83.8.98	exitoso
PC-B	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	exitoso
PC-B	S2, VLAN 4	Dirección	10.83.8.99.	exitoso
PC-B	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	exitoso

Figura 20. PING desde PC-A – hacia G0/0/1.20 - G0/0/1.30



Fuente: Autoría Propia.

Figura 21. PING desde PC-B – hacia G0/0/1.20 - G0/0/1.30



Fuente: Autoría Propia.

Con las pruebas hechas anteriormente se puede constatar que nuestra red es funcional y converge en su totalidad, los comandos PING ejecutados tanto para las interfaces configuradas con IPV4 como con IPV6 la respuesta es satisfactoria.

CONCLUSIONES

Con el desarrollo del presente documento se lleva a cabalidad las temáticas planteadas por el diplomado en profundización cisco; donde se coloca en práctica el conocimiento aprendido en temas de las telecomunicaciones, redes direccionamientos en un entorno práctico y sencillo.

Mediante el escenario se establece la importancia de la utilización de las temáticas abordadas durante el diplomado. El direccionamiento aplicado VLSM; se adecua a los rangos que se ajusten a lo que realmente es necesario. Las configuraciones de cada uno de los dispositivos es agregar aspectos que se necesitan para el debido funcionamiento y seguridad, garantizando responsabilidad de velar por la integridad de los datos de la organización que se está apoyando o en el entorno que se desarrollando el evento.

Respecto a las configuraciones en el escenario dos, se desarrollan los conocimientos adquiridos y uso de direccionamiento IPV4 como IPV6. Mediante la configuración de las VLANs se comprenden las diversas topologías planteadas de una forma virtual creadas dentro de una Red más grande que permite ordenar de manera Lógica los diferentes dispositivos de la misma, en las configuraciones y restricciones o aspectos de seguridad que le favorecen positivamente en el entorno que se esté trabajando; La configuraciones DHCP se asignan direcciones IP de manera dinámica dentro de un rango preestablecido llegando así a tener un detalle de conectividad exitosa.

BIBLIOGRAFIA.

FENG, W.C. A self-configuring RED gateway. En IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. {En linea}. (1999). {25 noviembre 2022}. Disponible en: https://ieeexplore.ieee.org/abstract/document/752150

FROOM, R., Frahim. CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. {En linea}. (2015). {13 octubre 2022}. Disponible en: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

MAESTRE, Javier. El derecho del nombre de dominio. {En línea}. (2001). {25 noviembre 2022}. Disponible en: https://books.google.com.co/books?hl=es&lr=&id=Dd4J0kwL1fcC&oi=fnd&pg=PA14&dq=MAESTRE,+Javier.+El+derecho+del+nombre+de+dominio.+(2001)&ots=7gVldH8nlM&sig=TdbPy8GBe0erBlIzuWEKjnDZA-o#v=onepage&q=MAESTRE%2C%20Javier.%20El%20derecho%20del%20nombre%20de%20dominio.%20(2001)&f=false

MAXWELL, Kim. Asymmetric digital subscriber line: Interim technology for the next forty years. IEEE Communications Magazine. {En línea}. (1996). {25 noviembre 2022}. Disponible en: https://ieeexplore.ieee.org/abstract/document/544330.

NAGAOKA, N.; AMETANI, A. A development of a generalized frequency-domain transient program-FTP. IEEE transactions on power delivery. {En linea}. (1988). {25 octubre 2022}. Disponible en: https://ieeexplore.ieee.org/abstract/document/194010

POSTEL, Jon. Internet control message protocol. {En linea}. (1981). {23 noviembre 2022}. Disponible en: https://www.rfc-editor.org/rfc/rfc792.html.

SINURAYA, Enda Wista. Teknik Variable Length Subnet Mask (Vlsm) Dan Virtual Local Area Network (Vlan). {En linea}. (2014). {25 OCtubre 2022}. Disponible en: https://ejournal.undip.ac.id/index.php/transmisi/article/view/9520

TEARE, D., VACHON, B., GRAZIANI, R. CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. {En linea}. (2015). {13 octubre 2022}. Disponible en: https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

ANEXOS

Anexo A: Descarga archivos de simulación:

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/an27ara903_unadvirtual_edu_co/EmWw-OGMTxJGvsWJBJQQ4tMBGM-yGRbxZnxuTDIIXpY1SQ?e=yTrTsi