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

ELIUD JULIO PINEDA

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

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

ELIUD JULIO PINEDA

Diplomado de opción de grado presentado para optar el título de Ingeniero de Sistemas

DIRECTOR:
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SANTA MARTA, 06 diciembre de 2022

AGRADECIMIENTOS

A Dios primeramente quien es la fuente de todo conocimiento, a mis padres y mis hermanas por su apoyo incondicional y por quienes soy la persona que soy hoy, a mi esposa por su comprensión, a cada uno de los tutores de las diferentes disciplinas quienes me formaron académicamente, y a todo el plantel de esta prestigiosa entidad la UNAD.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LAN (Local Área Networks, Redes de Área Local): Las redes LAN son de alcance limitado. Generalmente son redes privadas que están instaladas Redes Corporativas Redes de Datos dentro de un mismo edificio, oficina o campus. Su objetivo principal típicamente es compartir recursos (impresoras, discos, etc.). [1]

Protocolo TCP IP: TCP e IP son los protocolos más importantes. Su nombre representa al conjunto de protocolos que conforman la arquitectura formada por cinco niveles o capas:[2]

Router: Los routers analizan los datos que se van a enviar a través de una red, los empaquetan de forma diferente y los envían a otra red o a través de un tipo de red distinto.[3]

Hubs: Son elementos de red Ethernet que permiten conectar varios hosts en una red punto a punto[4]

UDP: (Protocolo de datagramas de usuario): El grupo de protocolos de Internet también maneja un protocolo de transporte sin conexiones, el UDP (User Data Protocol, protocolo de datos de usuario). El UDP ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto encapsulados sin tener que establecer una conexión.[5]

[1] JOSKOWICZ Jose Redes de Datos (2007)
[2] ESTRADA Adrian Protolos TCP/IP de Internet (2004)
[3] CISCO Systems, Inc. Conceptos generales (2012)
[4] LOPEZ Ricardo Enrrutamiento y configuración de redes (2018)
[5] MOLINA Carlos Fundamento de redes (2019)

RESUMEN

El avance de la electrónica en nuestro mundo ha dado a luz la ciencia de las redes de datos, estas se han convertido en una necesidad importante para todo tipo de empresas o instituciones que quieran optimizar su desempeño y gestión.

En este trabajo se desafían todas las habilidades y conocimientos adquiridos en el diplomado de profundización CISCO-CCNA para construir y diseñar protocolos de comunicación y enrutamiento desarrollando soluciones simuladas a los problemas planteados en los módulos de este curso.

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

ABSTRACT

The advance of electronics in our world has given birth to the science of data networks, these have become an important need for all types of companies or institutions that want to optimize their performance and management.

In this work, all the skills and knowledge acquired in the CISCO-CCNA in-depth diploma are challenged to build and design communication and routing protocols, developing simulated solutions to the problems raised in the modules of this course.

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

INTRODUCCIÓN

Durante el desarrollo del Diplomado de profundización CISCO se busca capacitar y entrenar en ambientes simulados la resolución de problemas relacionados con la implementación de redes LAN-WAN. En el siguiente trabajo desarrollaremos la solución de dos estudios de caso bajo el uso de tecnología CISCO

En el primer escenario se configurarán los dispositivos de una red pequeña. se realizará la configuración de un router, un switch y equipos pc, diseñaremos el esquema de direccionamiento IPv4 para las LAN propuestas. Teniendo en cuenta la administración segura de los dispositivos.

En el segundo escenario se configurarán los dispositivos de una red pequeña. Donde realizaremos la configuración de un router, un switch y equipos que deberán admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Por último, configuraremos un enrutamiento entre VLAN, DHCP, Etherchannel y port-security

1. DESARROLLO DEL ESCENARIO 1

Para este escenario se nos pide implementar la siguiente solución para una LAN pequeña, en donde debemos realizar primeramente el direccionamiento IP, Configurar los dispositivos intermedios (switch y router) garantizando la seguridad de los puertos y la conectividad exitosa entre dispositivos finales.

1.1. Topología

Figura 1: Topología escenario 1

Fuente: Prueba de habilidades ccna II 2022

Procedemos a realizar la construcción de la topología lógica en el simulador PACKET TRACER de acuerdo a la figura 1 implementamos el cableado e interconectamos los dispositivos

Figura 2: Construcción de la topología

Fuente: Autor

1.2. Direccionamiento IP

A continuación, en la tabla 1 se muestra el esquema de direccionamiento IP. Para la dirección IPv4 crearemos las dos subredes con la cantidad requerida de hosts. Asignaremos las direcciones de acuerdo con losrequisitos mencionados en la tabla de direccionamiento.

Tabla 1. Esquema de direccionamiento

ITEM	**REQUERIMIENTO**
DIRECCIÓN DE RED	172.70.3.0
Requerimiento de hostSubred LAN1	60
Requerimiento de hostSubred LAN2	20
R1 G0/0/1	172.70.3.62/26
R1 G0/0/0	172.70.3.158/27
S1 SVI	172.70.3.2/26
PC-A	172.70.3.10/26
PC-B	172.70.3.138/27

Fuente: Prueba de habilidades ccna II 2022

1.3. CONFIGURACION DE DISPOSITIVOS

1.3.1. Configuración del router

A continuación, se describe el paso a paso de la configuración inicial del router:

Router>

Router> enable	Ingresamos a modo privilegiado
Router# configure terminal	Ingresamos a modo de configuración
Router(config)# hostname R1	Asignamos nombre al Router
R1(config)# ip domain-name cisco-sa.com	Asignamos el nombre del dominio
R1(config)# enable secret ciscoenpass	Asignamos contraseña cifrada para el modo privilegiado
R1(config)# line console 0	Entramos al modo consola
R1(config-line)# password ciscoenpass	Establecemos contraseña a la consola
R1(config-line)# login	Hacemos la comprobación simple de la contraseña en consola
R1(config-line)# exit	Salimos del modo consola
R1(config)# security passwords min-length 10	Establecemos longitud mínima para las contraseñas de 10

	caracteres
R1(config)# username admin secret admin1pass	Creamos el usuario admin y le asignamos la contraseña admin1pass
R1(config)# line vty 0 15	Entramos a la línea de terminal virtual
R1(config-line)# login local	Configuramos el inicio de sesión en las lineas VTY con la base de datos local
R1(config-line)# transport input ssh	Configuramos las líneas VTY para que acepten únicamente las conexiones SSH
R1(config-line)# exit	Salimos del modo line VTY
R1(config)# service pasword-encrytion	Ciframos las contraseñas de texto no cifrado
R1(config)# banner motd %R1 Configurado por Eliud Josue Julio Pineda del Programa de Ingenieria de Sistemas UNAD%	Configuramos un banner MOTD
R1(config)# interface g0/0/1	Entramos al modo interface para configurar el puerto g0/0/1
R1(config-if)# description Conectar a la LAN1	Asignamos una descripción
R1(config-if)# ip address 172.70.3.62 255.255.255.128	Establecemos dirección IPv4 y Mascara de sub red

R1(config-if)# no shutdwon	Activamos la interface
R1(config-if)# exit	Salimos de la interface g0/0/1
R1(config)# interface g0/0/0	Entramos al modo interface para configurar el puerto g0/0/0
R1(config-if)# description Conectar a la LAN2	Asignamos una descripción
R1(config-if)# ip address 172.70.3.158 255.255.255.192	Establecemos dirección IPv4 y Mascara de sub red
R1(config-if)# no shutdwon	Activamos la interface
R1(config-if)# exit	Salimos de la interface g0/0/0
R1(config)# crypto key generate rsa R1(config)# How many bits in the modulus (512): 1024	Generamos una clave de cifrado rsa con un modulo de 1024 bits
R1(config)# exit	Salimos del modo configuración

1.3.2. Configuracion del switch

Una vez configurado el router procedemos a configurar el switch en la interfaz de línea de comando (CLI).

Switch> enable	Ingresamos a modo privilegiado
Switch# configure terminal	Ingresamos a modo de configuración

Switch(config)# no ip domain lookup	Desactivamos la búsqueda de DNS
Switch(config)# hostname S1	Asignamos el nombre de S1 al Swicth
S1(config)# ip domain-name ccna-sa.com	Establecemos un nombre de dominio
S1(config)# enable secret ciscoenpass	Asignamos contraseña cifrada para el modo privilegiado
S1(config)# line console 0	Entramos al modo consola
S1(config-line)# password ciscoenpass	Establecemos contraseña a la consola
S1(config-line)# login	Hacemos la comprobación simple de la contraseña en consola
S1(config-line)# exit	Salimos del modo consola
S1(config)# interface range f0/1-4, f0/7-24, g0/1-2	Seleccionamos los siguientes rangos de puertos del 1 al 4, del 7 al 24, y el 1 y el 2 de la interface g0
S1(config-if-range)# shutdown	Desactivamos los puertos seleccionados
S1(config-if-range)# exit	Salimos del modo rango de interface
S1(config)# username admin secret admin1pass	Creamos el usuario admin y le asignamos la contraseña admin1pass
S1(config)# line vty 0 15	Entramos a la línea de terminal virtual
S1(config-line)# login local	Configuramos el inicio de sesión en las lineas VTY con la base

	de datos local
S1(config-line)# transport input ssh	Configuramos las líneas VTY para que acepten únicamente las conexiones SSH
S1(config-line)# exit	Salimos del modo line VTY
S1(config)# service pasword-encrytion	Cifamos las contraseñas de texto no cifrado
S1(config)# banner motd %S1 Configurado por Eliud Josue Julio Pineda del Programa de Ingenieria de Sistemas UNAD%	Configuramos un banner MOTD
S1(config)# crypto key generate rsa S1(config)# How many bits in the modulus ¨(512): 1024	Generamos una clave de cifrado rsa con un módulo de 1024 bits
S1(config)# interface vlan 1	Entramos a la interface vlan 1
S1(config-if)# description VLAN 1 del S1 en la LAN1	Asignamos una descripción
S1(config-if)# ip address 172.70.3.2 255.255.255.192	Establecemos dirección IPv4 y Mascara de Sub Red
S1(config-if)# no shutdown	Activamos la interface vlan 1
S1(config)# exit	Salimos del modo interface vlan 1
S1(config)#	

1.3.3. Configuración del equipo PC-A

Realizamos la asignación de dirección IPv4, dirección física o MAC, mascara de subred y puerta de enlace; en el equipo denominado PC-A, esto realizamos mediante el comando de consola **ipconfig /all**

Tabla 2: Configuración del PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	0010.1164.B395
Dirección IPv4	172.70.3.10
Máscara de subred	255.255.255.128
Puerta de enlace IPv4 predeterminada	172.70.3.62

Fuente: Prueba de habilidades ccna II 2022

1.3.4. Configuración del equipo PC-B

Realizamos la asignación de dirección IPv4, dirección física o MAC, mascara de subred y puerta de enlace; en el equipo denominado PC-A, esto realizamos mediante el comando de consola **ipconfig /all**

Tabla 3: Configuración del PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000A.411E.D151
Dirección IPv4	172.70.3.138
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.70.3.158

Fuente: Prueba de habilidades ccna II 2022

1.3.5. Verificación de conectividad de extremo a extremo

Utilizaremos el comando ping en la ventana de CMD de windows para probar la conectividad entre todos los dispositivos de red, los resultados de estos los observamos en la siguiente tabla:

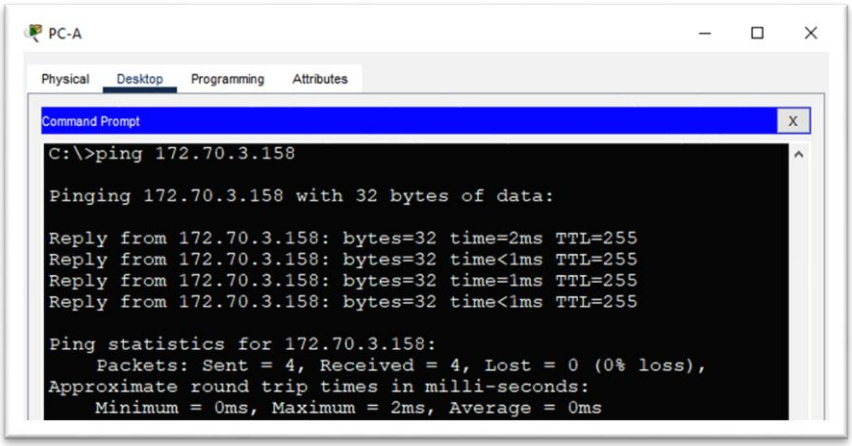
Tabla 4: Resultados de prueba de conectividad

Desde	**A**	**Dirección IP**	**Resultados de ping**
PC-A	R1 G0/0/0	172.70.3.158	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.70.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S1 VLAN 1	172.70.3.2	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	PC-B	172.70.3.138	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
PC-B	R1 G0/0/0	172.70.3.158	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	R1 G0/0/1	172.70.3.62	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
	S1 VLAN1	172.70.3.2	Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Fuente: Prueba de habilidades ccna II 2022

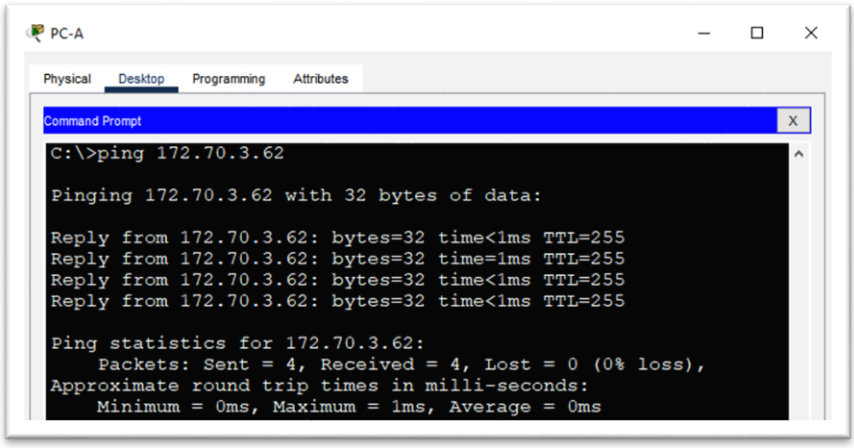
1.3.6. Evidencias de pruebas de conectividad

Figura 3: Ping de PC-A a R1 G0/0/0



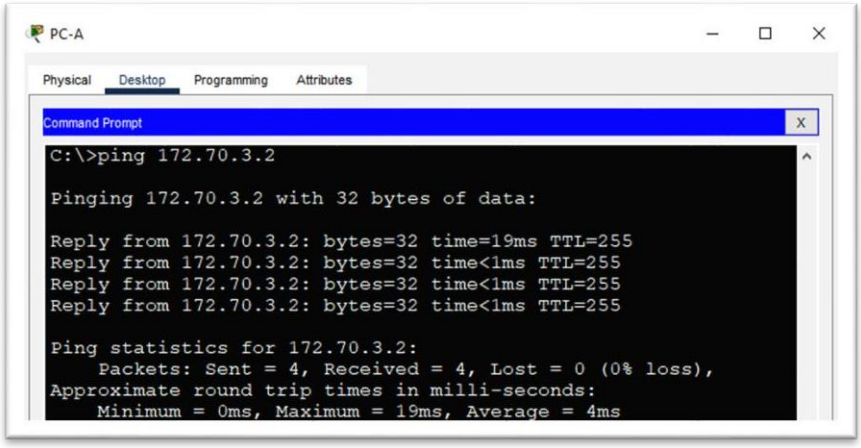
Fuente: Autor

Figura 4: Ping de PC-A a R1 G0/0/1



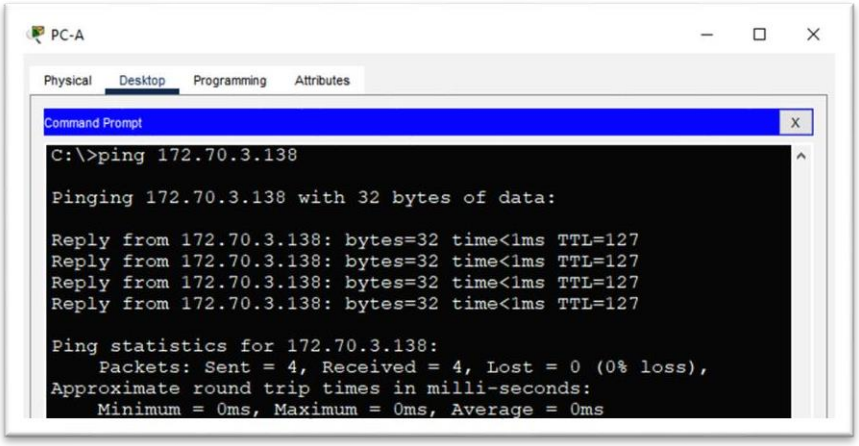
Fuente: Autor

Figura 5: Ping de PC-A a S1 VLAN 1



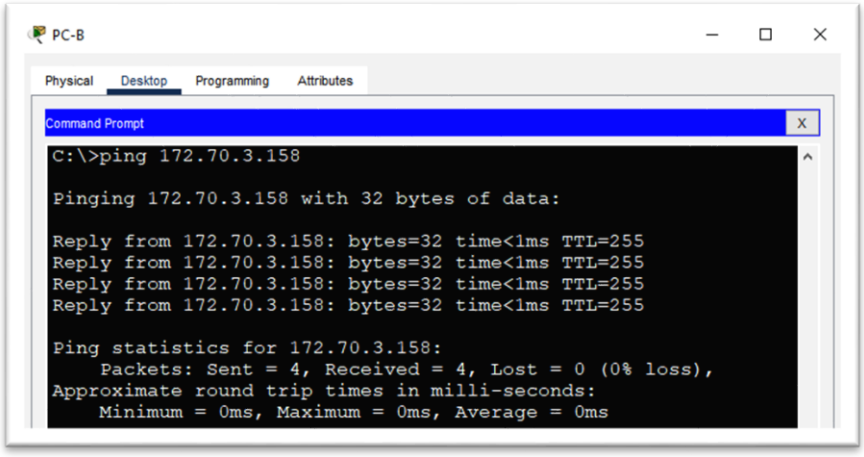
Fuente: Autor

Figura 6: Ping de PC-A a PC-B



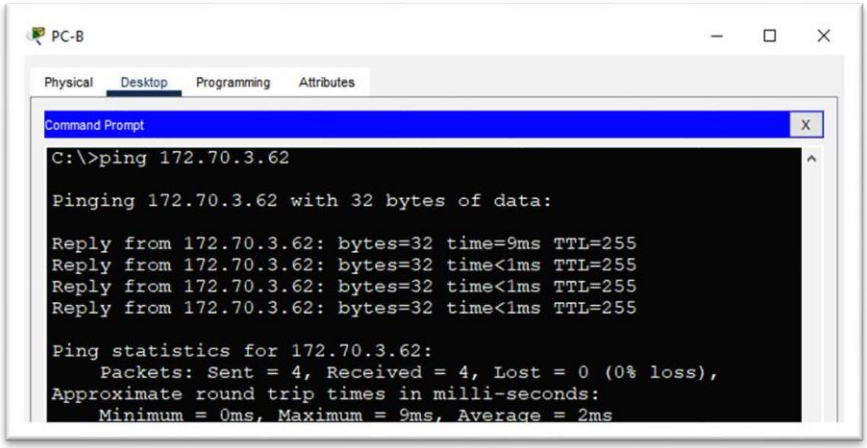
Fuente: Autor

Figura 7: Ping de PC-B a R1 G0/0/0



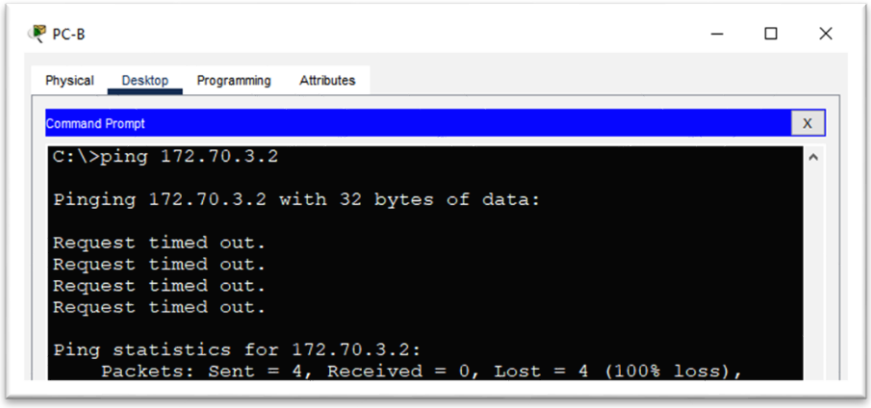
Autor: Fuente

Figura 8: Ping de PC-B a R1 G0/0/1



Fuente: Autor

Figura 9: Ping de PC-A a S1 VLAN 1



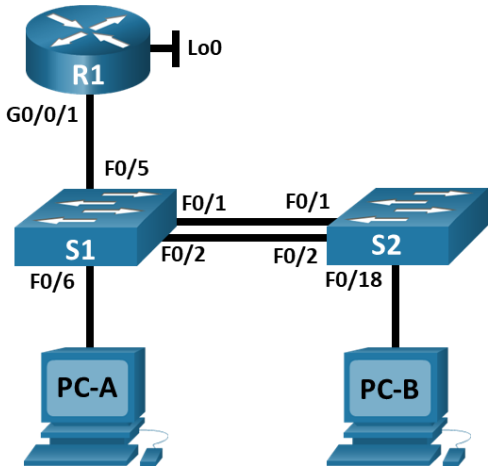
Autor: Fuente

2. DESARROLLO DEL ESCENARIO 2

2.1. Topología

En este segundo escenario se configurarán los dispositivos de una red pequeña, para esto debemos realizar las configuraciones necesarias en cada uno de los dispositivos que conforman esta red: un router, un switch y equipos que deben admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Tambien realizaremos el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

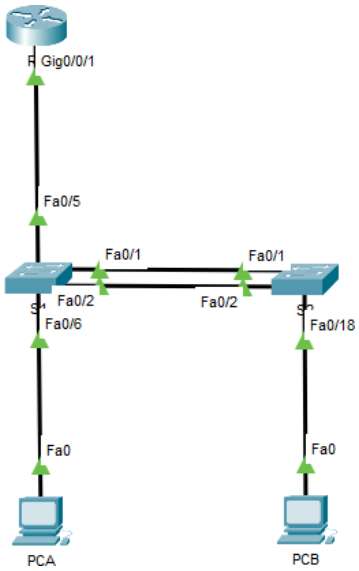
Figura 10: Topología escenario 2



Fuente: Prueba de habilidades ccna II 2022

Procedemos a realizar la construcción de la topología lógica en el simulador PACKET TRACER de acuerdo a la figura 10 implementamos el cableado e interconectamos los dispositivos

Figura 11: Construcción de la topología



A continuación, se describen los requerimientos para las redes virtuales VLAN que deben ser configuradas de manera lógica en el router y los switch's:

Tabla 5: Listado de VLANs a crear

VLAN	**NOMBRE DE LA VLAN**
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Prueba de habilidades ccna II 2022

2.2. Direccionamiento IP

A continuación, se nos muestra el esquema de direccionamiento que debemos aplicar a cada interfaz de los dispositivo, teniendo en cuenta que no debe haber ninguna interfaz en el router que admita VLAN 50, para esto debemos realizar la asignación de IP aplicando el protocolo IPv4 y protocolo IPV6.

Tabla 6: Esquema de direccionamiento IPv4 - IPv6

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.70.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.70.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.70.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 40	10.70.8.98 /29	10.70.8.97
	2001:db8:acad:c: :98 /64	No corresponde

	fe80: :98	No corresponde
S2 VLAN 40	10.70.8.99 /29	10.70.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace default IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Prueba de habilidades ccna II 2022

2.3. CONFIGURACION DE DISPOSITIVOS

2.3.1. Inicialización de dispositivos

Para empezar a configurar los dispositivos que conforman nuestra red debemos borrar las configuraciones de inicio y las VLAN tanto router como en cada uno de los switch's y volvemos a cargar los dispositivos mediante el comando reload.

Router>enable

Router#delete vlan.data

Delete filename [vlan.data]?

Delete flash:/vlan.data? [confirm]

%Error deleting flash:/vlan.data (No such file or directory)

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Switch>enable

Switch#delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:/vlan.dat? [confirm]

%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
System configuration has been modified. Save? [yes/no]:no
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00E0.A346.5AC5
Xmodem file system is available

2.3.2. Habilitación de protocolo IPv6 en dispositivos

Después de haber inicializado y recargado los dispositivos procedemos a configurar la plantilla SDM en cada uno de los switch's para que nos permita hacer la asignación de direcciones IPv6 y volvemos a cargar los dispositivos para que nos tome la nueva configuración.

.

Switch(config)#sdm prefer ?
default Default bias
dual-ipv4-and-ipv6 Support both IPv4 and IPv6

lanbase-routing Lanbase routing
qos Qos bias

Switch(config)#sdm prefer dual-ipv4-and-ipv6 ?
default Default bias

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

Switch#reload

Switch>enable

Switch#sh sdm prefer
The current template is "dual-ipv4-and-ipv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 1024 VLANs.

2.3.3. Configuraciones básicas del router

En este paso realizaremos las configuraciones basicas del router, las cuales consisten en: Desactivar la búsqueda DNS, darle uel nombre de R1 al router, asignar un nombre de dominio, establecer la contraseña **class** para el modo privilegiado, y la contraseña de **cisco** para el acceso a la consola, establecer una longitud para las contraseñas de mínimo 5 caracteres, crear el usuario

administrativo “admin” en labase de datos local con el password de **admin1pass,** configurar el inicio de sesión en las líneas VTY para que use la base de datos local, configurar VTY solo aceptando SSH, cifrar las contraseñas de texto no cifrado y por ultimo configuraremos un MOTD Banner con el nombre del dispositivo seguido del nombre del estudiante y el programa al que pertenece

```
Router>enable
Router(config)#no ip domain-lookup
Router (config)#hostname R1
R1(config)#ip domain-name ccna-sa.com
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 5
R1(config)#username admin privilege 15 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1#banner motd "R1 - ELIUD JULIO - ING DE SISTEMAS"
R1(config-line)#exit
R1(config)#exit
```

2.3.4. Configuración de interfaces y subinterfaces del router

Una vez configurado los aspectos básicos del router procedemos a realizar las configuraciones de interfaz y subinterfaces en este dispositivo según la tabla de direccionamiento, estableceremos la dirección IPv4, la dirección IPv6, también estableceremos la dirección local de enlace IPv6 como **fe80::1** y por ultimo activaremos la interfaz.

R1: ELIUD JULIO P. - ING. DE SISTEMAS

User Access Verification

Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1
R1(config)#int g0/0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.70.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#int g0/0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.70.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64

```
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 10.70.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.56
R1(config-subif)#encapsulation dot1Q 56
R1(config-subif)#exit

R1(config)#int g0/0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#int g0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20,
changed state to up
```

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.40, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.60, changed state to up

2.3.5. Configuracion del loopback 0

Después de haber configurado las interfaces y subinterfaces del router procedemos a realizar la configuración del loopback Estableciendo la dirección IPv4 y la dirección IPv6, asignando la dirección local de enlace IPv6 como **fe80::1**, y por ultimo configuraremos una clave de cifrado RSA con modulo de 1024 bits

R1(config)#interface loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#interface loopback 0
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 4:16:36.27: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#

2.3.6. Configuración básica del Switch 1

Una vez realizada la configuración de la interfaz lookback-0 procedemos efectuar las configuraciones básicas en ambos switch's, la cual comprende las siguientes acciones: Desactivar la búsqueda DNS, establecer el nombre de **S1** al dispositivo, asignar el nombre de dominio **ccna-sa.com**, establecer la contraseña **class** para el modo privilegiado y para el acceso de consola estableceremos la contraseña **cisco**, crearemos un usuario administrativo en la base de datos local con nombre de usuario **admin** y password **admin1pass**, configuraremos el inicio de sesión en las líneas VTYpara que use la base de datos local y para que acepten únicamente las conexiones SSH, Cifraremos las contraseñas de texto no cifrado, configuraremos un MOTD Banner con el nombre del dispositivo, nombre del estudiante y el programa al que pertenece y por ultimo generaremos una clave de cifrado RSA con modulo de 1024 bits.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-sa.com
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
```

```
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "S1: ELIUD JULIO P. - ING DE SISTEMAS"
S1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S1.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 3:26:51.957: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

2.3.7. Configuraciòn bàsica del Switch 2

Una vez realizada la configuración básica en el switch 1 procedemos a realizar la configuración del switch 2 bajo los mismos parámetros del switch 1.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#ip domain-name ccna-sa.com
S2(config)#enable secret class
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
```

S2(config)#username admin privilege 15 secret admin1pass
S2(config)#line vty 0 4
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd "S2: ELIUD JULIO P. - ING DE SISTEMAS"
S2(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S2.ccna-sa.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 3:16:5.411: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#

2.3.8. Configuración VLAN 40 en S1

En este punto realizaremos la Configuración de la interfaz de administración (SVI) para el switch **S1**, habilitando la interfaz VLAN 40. Para esto debemos realizar los siguientes pasos: establecer la dirección IPv4 de capa 3, establecer la dirección local de enlace IPv6 como **FE80: :98**, establecer la dirección IPv6 de capa 3 y por último establecer la puerta de enlace predeterminada como **10.70.8.97** para IPv4.

S1: ELIUD JULIO P. - ING DE SISTEMAS

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 40
S1(config-if)#ip address 10.70.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#exit
S1(config)#ip default-gateway 10.70.8.97
S1(config)# no shutdown

2.3.9. Configuración VLAN 40 en S2

De igual manera realizaremos la Configuración de la interfaz de administración (SVI) para el switch **S2**, habilitando la interfaz VLAN 40. bajo los mismos parámetros realizados en el switch **S1**: estableciendo la dirección IPv4 de capa 3, la dirección local de enlace IPv6 como **FE80: :99** y Establecer la dirección IPv6 de capa 33 y por último establecer la puerta de enlace predeterminada como **10.70.8.97** para IPv4.

S2: ELIUD JULIO P. - ING DE SISTEMAS

User Access Verification

Password:

S2>enable
Password:
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#ipv6 unicast-routing
S2(config)#interface vlan 40
S2(config-if)#ip address 10.70.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#exit
S2(config)#ip default-gateway 10.70.9.97
S2(config)#no shutdown

2.4. CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

A continuación, debemos crear un enlace en uno o más puertos de los switch's para permitir el paso del tráfico de las distintas VLANs que también crearemos en este paso. este enlace debe permitir la conexión entre los switch's S1 y S2 y del switch S1 al R1. Esto nos evita la necesidad de utilizar un enlace físico para cada VLAN.

2.4.1. Creacion de las VLAN's en el S1

La configuración del S1 incluye las siguientes tareas: Crear la VLAN 20 de nombre Docentes, VLAN 30,de nombre estudiantes, VLAN 40 de nombre invitados, VLAN 50, de nombre usuarios, VLAN 56, esta última será nuestra VLAN nativa.

S1: ELIUD JULIO P. - ING DE SISTEMAS

User Access Verification

Password:

S1>enable
Password:
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 20

```
S1(config-vlan)#name Docentes
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Estudiantes
S1(config-vlan)#exit
S1(config)#vlan 40
S1(config-vlan)#name Invitados
S1(config-vlan)#exit
S1(config)#vlan 50
S1(config-vlan)#name Usuarios
S1(config-vlan)#exit
S1(config)#vlan 56
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#exit
```

Figura 12: Verificación de creación de VLAN's en S1

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
20   Docentes                         active
30   Estudiantes                      active
40   Invitados                        active
50   Usuarios                         active
56   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

Fuente: Autor

2.4.2. Configuración “TRUNK” 802.1Q en S1

Esta configuración debemos hacerla en las siguientes interfaces: F0/1, F0/2 y F0/5 para que utilicen la VLAN 56 NATIVA como troncal principal de tráfico de datos.

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

S1(config)#int f0/2
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 56
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 56
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56

Para comprobar que efectivamente se ha configurado estas interfaces haremos uso del comando **show interface f0/x switchport** como se muestra a continuación:

S1#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
Voice VLAN: none

S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk

Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
Voice VLAN: none

S1#show interface f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
Voice VLAN: none

2.4.3. Creación de un grupo de puertos en S1

Después de esto crearemos un grupo de puertos etherchannel de capa 2 para que utilicen las interfaces F0/1 y F0/2

S1(config)#int range f0/1-2
S1(config-if-range)#channel-group 1 mode active

S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

S1(config-if-range)#exit
S1(config)#int port-channel 1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S1(config-if)#exit

2.4.4. Configuración de acceso de PC-A a VLAN 20 en S1

En este punto debemos permitir el acceso al puerto F0/6 a la VLAN 20 del Switch S1. Este puerto nos comunica con el PC-A según la topología.

S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S1(config-if)#exit
S1(config)#int f0/6
S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#exit

S1(config)#exit

S1#

Figura 13: Verificación de asignación del puerto Fa0/6 en S1

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
20   Docentes                         active    Fa0/6
30   Estudiantes                      active
40   Invitados                        active
50   Usuarios                         active
56   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Fuente: Autor

2.4.5. Seguridad de puertos en S1

Debemos proteger el puerto de acceso F0/6 con un numero máximo de 4 direcciones MAC

S1(config)#int f0/6

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security maximum 4

S1(config-if)#switchport port-security violation shutdown

S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#exit

S1(config)#exit

De igual manera también debemos proteger todas las interfaces no utilizadas redireccionándolas hacia la VLAN 50 y desactivando dichas interfaces.

```
S1(config)#interface range g0/1-2, f0/3-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#shutdown
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#exit
```

2.4.6. Creación de las VLAN’s en el S2

La configuración del S2 incluye las siguientes tareas: Crear la VLAN 20 de nombre Docentes, VLAN 30,de nombre estudiantes, VLAN 40 de nombre invitados, VLAN 50, de nombre usuarios, VLAN 56, esta ultima será nuestra VLAN nativa.

S1: ELIUD JULIO P. - ING DE SISTEMAS

User Access Verification

Password:

S2>enable
Password:
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config-vlan)#exit
S2(config)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config-vlan)#exit
S2(config)#vlan 40
S2(config-vlan)#name Invitados
S2(config-vlan)#exit
S2(config)#vlan 50
S2(config-vlan)#name Usuarios
S2(config-vlan)#exit
S2(config)#vlan 56
S2(config-vlan)#name Native

S2(config-vlan)#exit

S2(config)#exit

Figura 14: Verificación de creación de VLAN's en S2

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
20   Docentes                         active
30   Estudiantes                      active
40   Invitados                        active
50   Usuarios                         active
56   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

Fuente: Autor

2.4.7. Configuración “TRUNK” 802.1Q en S2

Esta configuración debemos hacerla en las interfaces F0/1 y F0/2 para que utilicen la VLAN 56 NATIVA como troncal principal de tráfico de datos.

S2(config)#int f0/1

S2(config-if)#switchport mode trunk

S2(config-if)#switchport trunk native vlan 56

S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56

S2(config-if)#exit

S2(config)#int f0/2

S2(config-if)#switchport mode trunk

S2(config-if)#switchport trunk native vlan 56

S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S2(config-if)#exit

Para comprobar que efectivamente se ha configurado estas interfaces haremos uso del comando **show interface f0/x switchport** como se muestra a continuación:

S2#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
Voice VLAN: none

S2#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On

Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
Voice VLAN: none

2.4.8. Creación de un grupo de puertos en S2

Después de esto crearemos un grupo de puertos etherchannel de capa 2 para que utilicen las interfaces F0/1 y F0/2.

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

S2(config-if-range)#exit
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S2(config-if)#exit
S2(config)#exit

2.4.9. Configuración de acceso de PC-B a VLAN 30 en S2

En este punto debemos permitir el acceso al puerto F0/18 a la VLAN 30 del Switch S2. Este puerto nos comunica con el PC-B según la topología.

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#exit
S2(config)#exit

Figura 15: Verificación de asignación del puerto Fa0/18 en S2

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
20   Docentes                         active
30   Estudiantes                      active    Fa0/18
40   Invitados                        active
50   Usuarios                         active
56   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Fuente Autor

2.4.10. Seguridad de puertos en S2

Debemos proteger el puerto de acceso F0/18 con un número máximo de 4 direcciones MAC

S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 4
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#

De igual manera también debemos proteger todas las interfaces no utilizadas enviandolas hacia la VLAN 50 y desactivando dichas interfaces.

```
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range g0/1-2, f0/3-17, f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#shutdown
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#exit
S2(config)#exit
```

3. CONFIGURACIÒN DE DHCP

En este punto debemos establecer el default routing realizando la creación de unas rutas predeterminadas para IPv4 e IPv6 que dirijan el trafico a la interfaz loopback 0.

3.1. Configuración IPv4 DHCP para VLAN20

Crearemos un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asignaremos el nombre de dominio ccna-sa.net yestableceremos la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan20
R1(dhcp-config)#network 10.70.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.70.8.1
R1(dhcp-config)#domain-name ccna-sa.net
R1(dhcp-config)#ip dhcp excluded-address 10.70.8.2 10.70.8.51
R1(config)#
```

3.2. Configuración IPv4 DHCP para VLAN30

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan30
R1(dhcp-config)#network 10.70.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.70.8.65
R1(dhcp-config)#domain-name ccna-sb.net
R1(dhcp-config)#ip dhcp excluded-address 10.70.8.66 10.70.8.83
R1(config)#exit
```

3.3. Configuración de Servidores

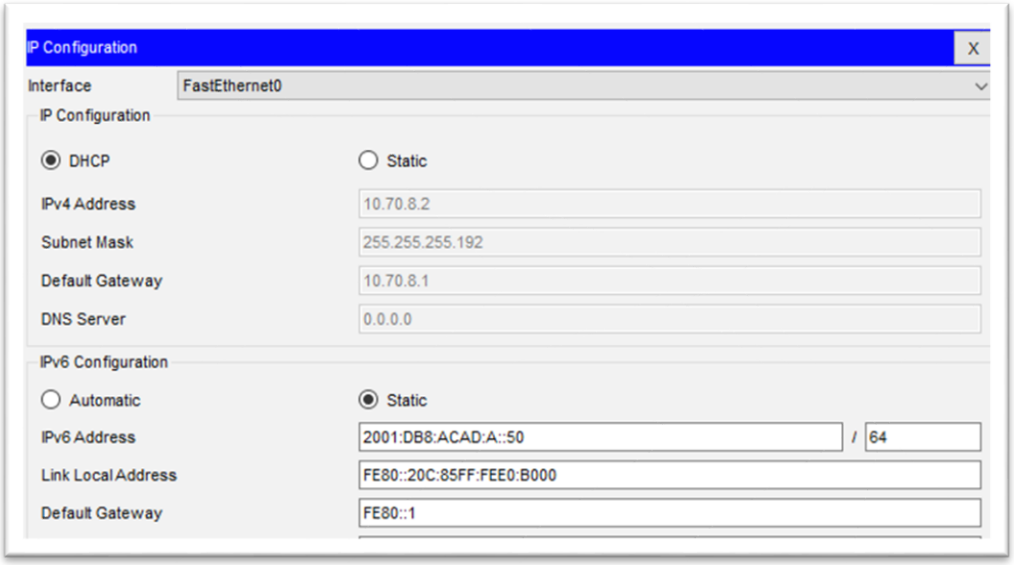
Seguidamente configuraremos los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asignaremos estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor y mediante el comando **ipconfig /all**. Registraremos los resultados de conectividad en la siguiente tabla.

Tabla 7: Configuración de PC-A

Configuración de red de PC-A	
Descripción	Equipo PC-A
Dirección física	000C.85E0.B000
Dirección IP	10.70.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.70.8.1
Gateway predeterminado IPv6	FE80::1

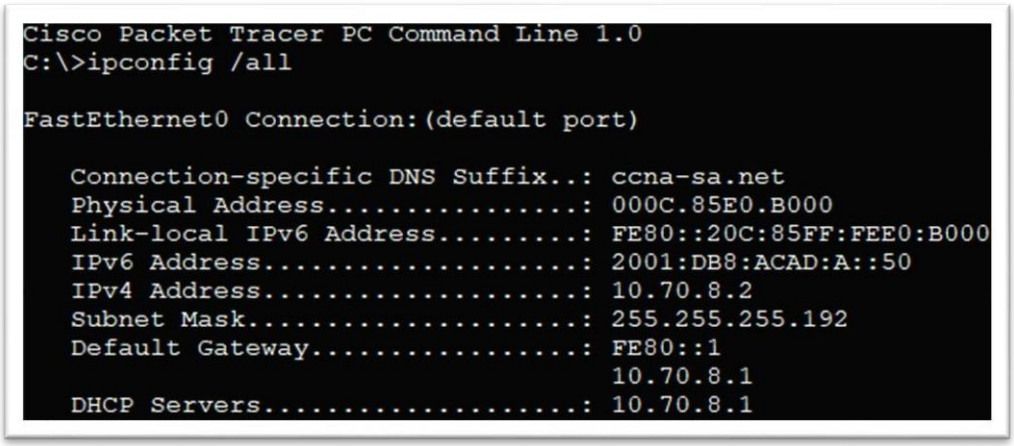
Fuente: Prueba de habilidades ccna II 2022

Figura 16: Configuración de DHCP para IPv4 y dirección estática para IPv6 - PC-A



Fuente: Autor

Figura 17: Evidencia de configuracion de IP por comando de consola en PC-A.



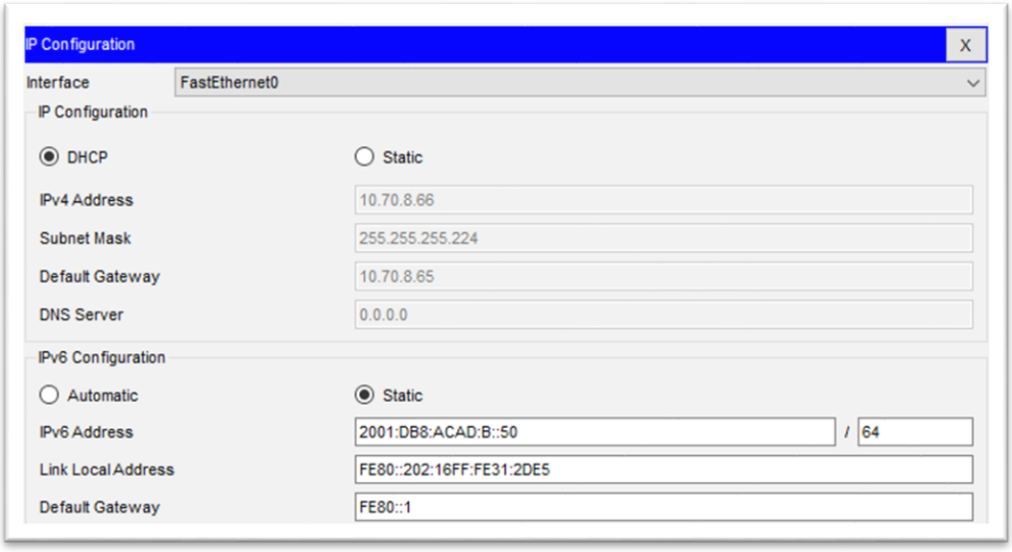
Fuente: Autor

Tabla 8: Configuración de PC-B

Configuración de red de PC-B	
Descripción	Equipo PC-B
Dirección física	0002.1631.2DE5
Dirección IP	10.70.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.70.8.65
Gateway predeterminado IPv6	FE80::1

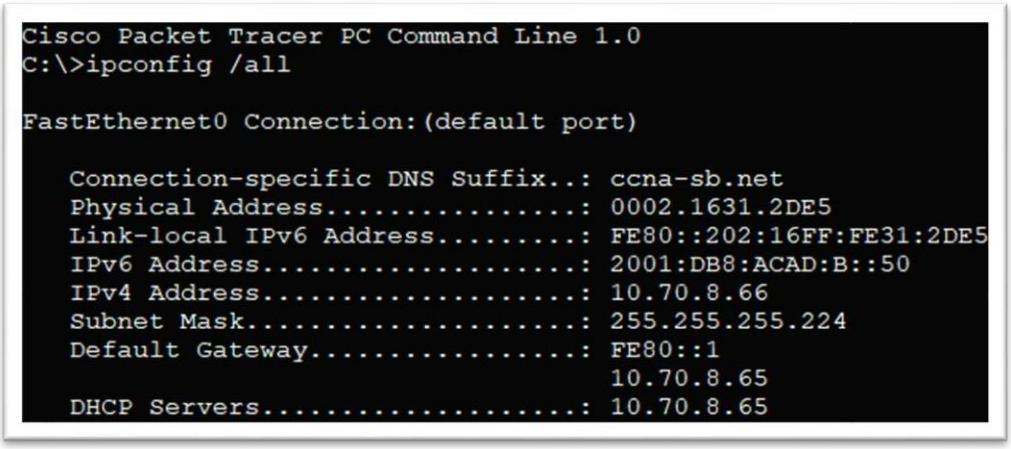
Fuente: Prueba de habilidades ccna II 2022

Figura 18: Configuración de DHCP para IPv4 y dirección estática para IPv6 - PC-B



Fuente: Autor

Figura 19: Evidencia de configuración de IP por comando de consola en PC-B



Fuente: Autor

3.4. Verificación de conectividad de extremo a extremo

Haciendo uso del comando ping realizaremos las pruebas de conectividad IPv4 e IPv6 entre todos los dispositivos de red tomando como guía la siguiente tabla registraremos los resultados de cada ping.

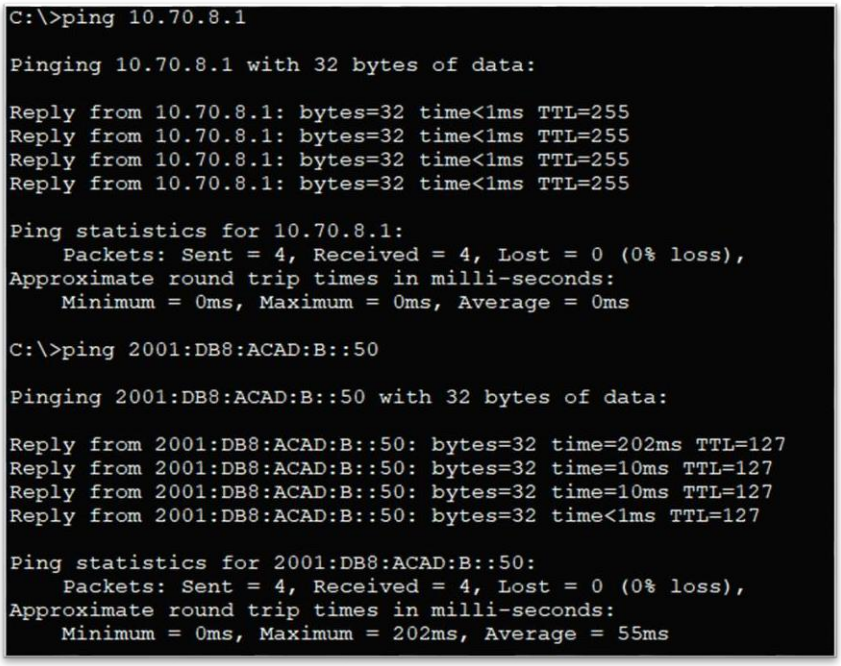
Tabla 9: Resultados de verificación de conectividad

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.70.8.1	Exitoso
		IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.30	IPv4	10.70.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.40	IPv4	10.70.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 40	IPv4	10.70.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98	Falló
	S2, VLAN 40	IPv4	10.70.8.99.	Exitoso
		IPv6	2001:db8:acad:c: :99	Falló
	PC-B	IPv4	10.70.8.66	Exitoso
		IPv6	2001:DB8:ACAD:B::50	Exitoso
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1	Exitoso
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1	Exitoso
	R1, G0/0/1.20	IPv4	10.70.8.1	Exitoso

		IPv6	2001:db8:acad:a: :1	Exitoso
	R1, G0/0/1.30	IPv4	10.70.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.40	IPv4	10.70.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 40	IPv4	10.70.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98	Falló
	S2, VLAN 40	IPv4	10.70.8.99	Exitoso
		IPv6	2001:db8:acad:c: :99	Falló

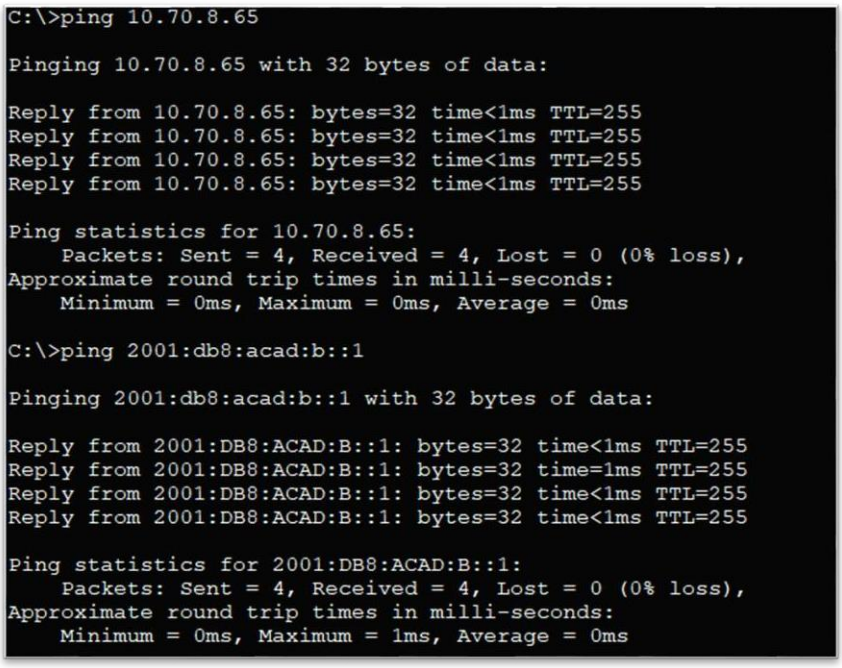
Fuente: Prueba de habilidades ccna II 2022

Figura 20: Resultado ping de PC-A a R1, G0/0/1.20 IPv4 e IPv6



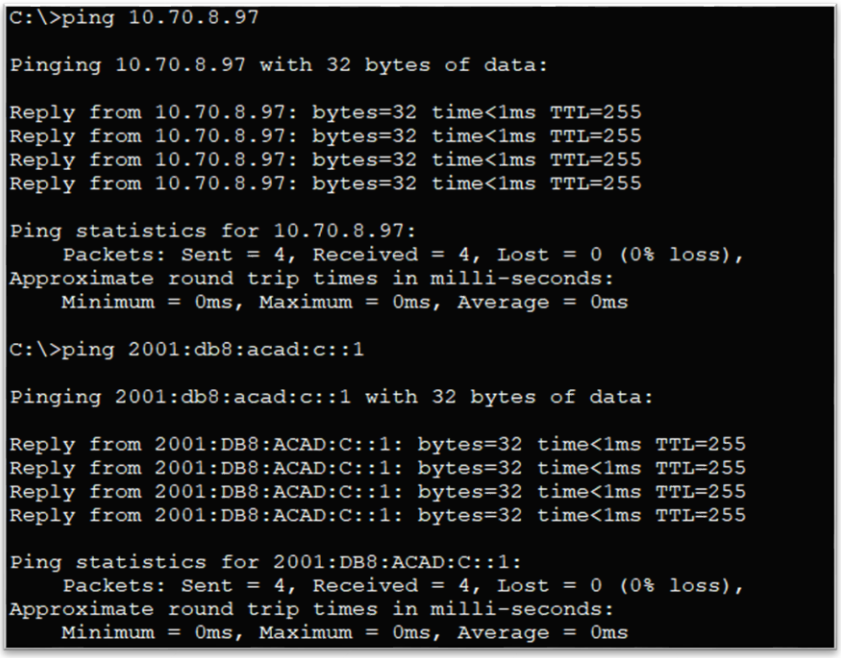
Fuente: Autor

Figura 21:Resultado ping de PC-A a R1, G0/0/1.30 IPv4 e IPv6



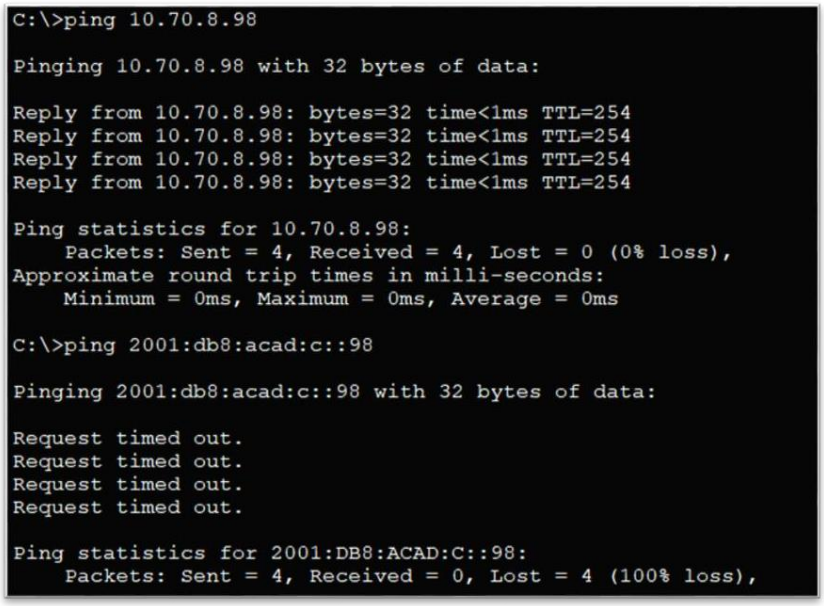
Fuente: Autor

Figura 22: Resultado ping de PC-A a R1, G0/0/1.40 IPv4 e IPv6



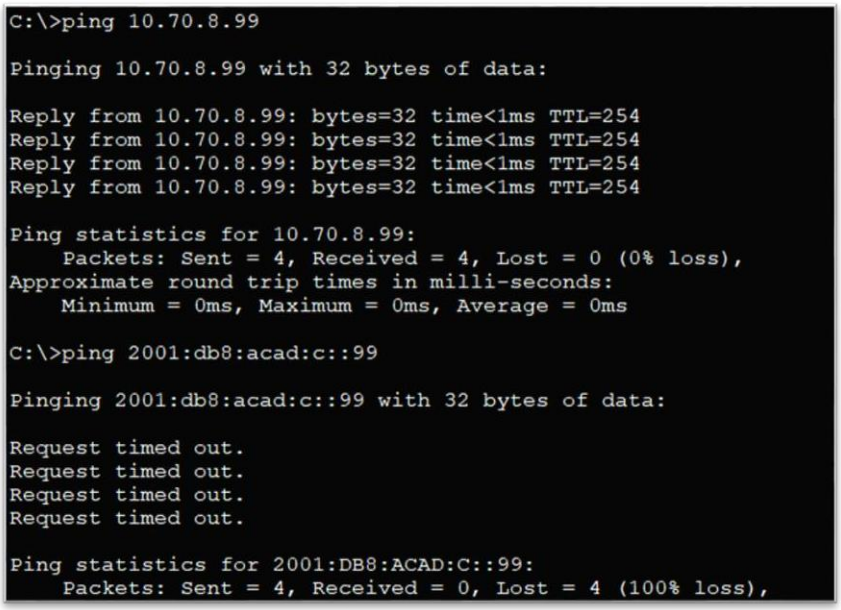
Autor: Fuente

Figura 23: Resultado ping de PC-A a S1, VLAN 40 IPv4 e IPv6



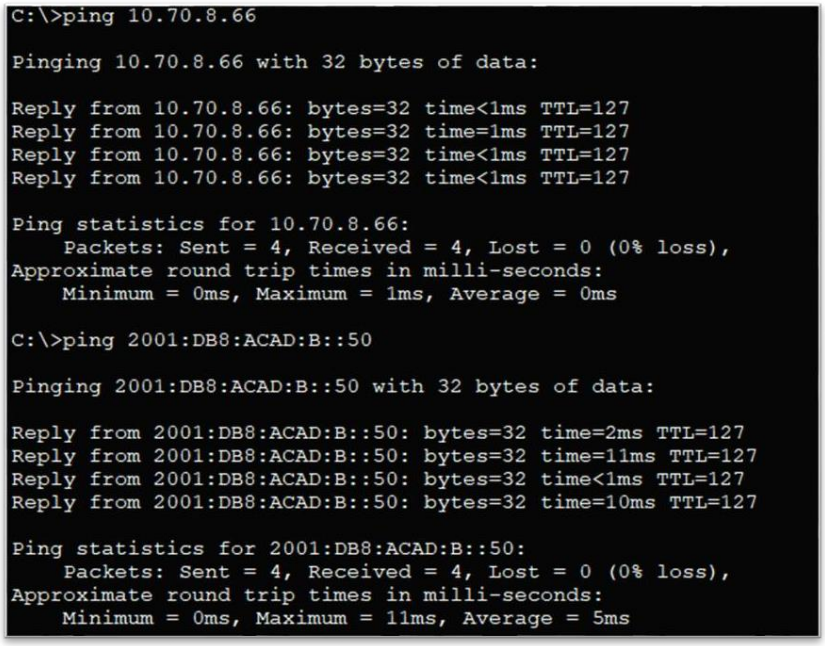
Fuente: Autor

Figura 24: Figura 23: Resultado ping de PC-A a S2, VLAN 40 IPv4 e IPv6



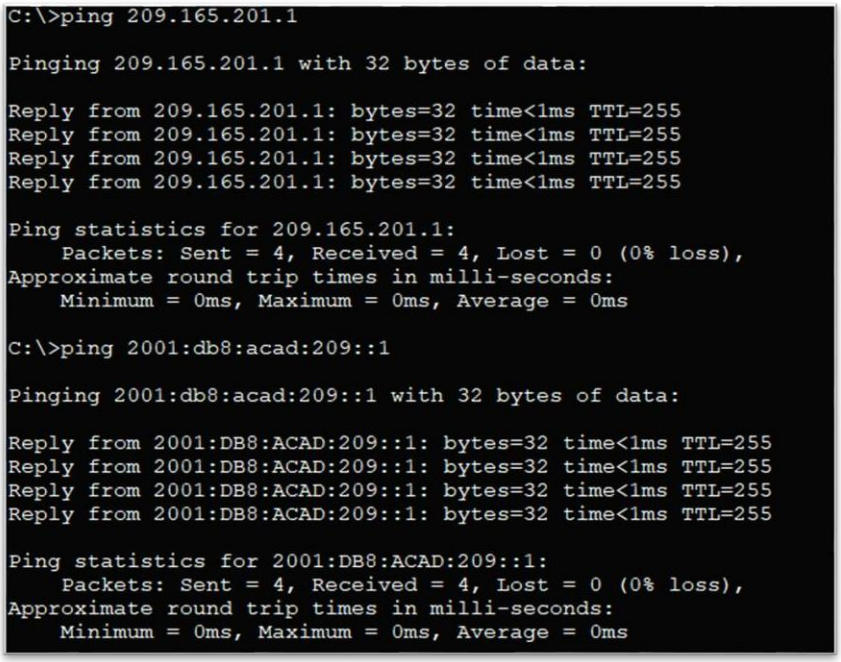
Fuente: Autor

Figura 25: Resultado ping de PC-A a PC-B IPv4 e IPv6



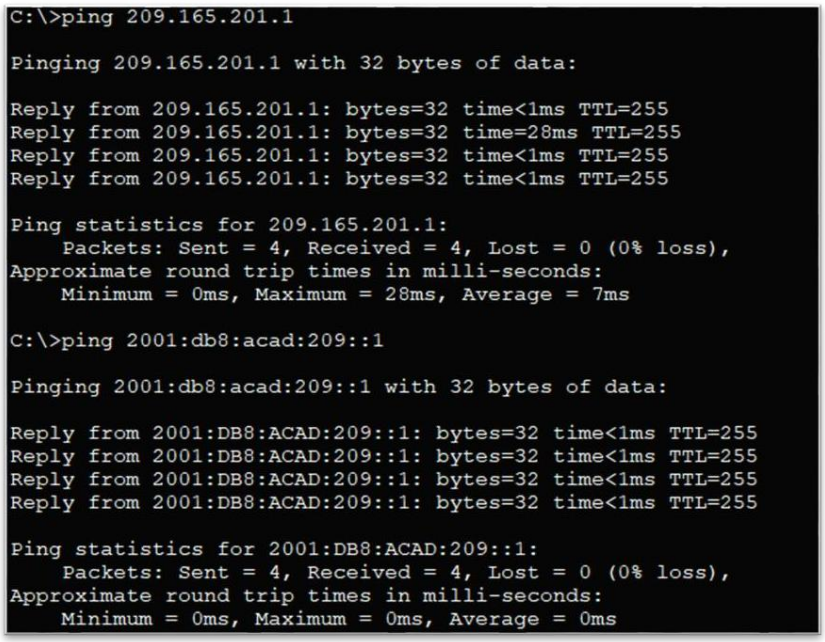
Fuente: Autor

Figura 26: Resultado ping de PC-A a R1 Bucle 0 IPv4 e IPv6



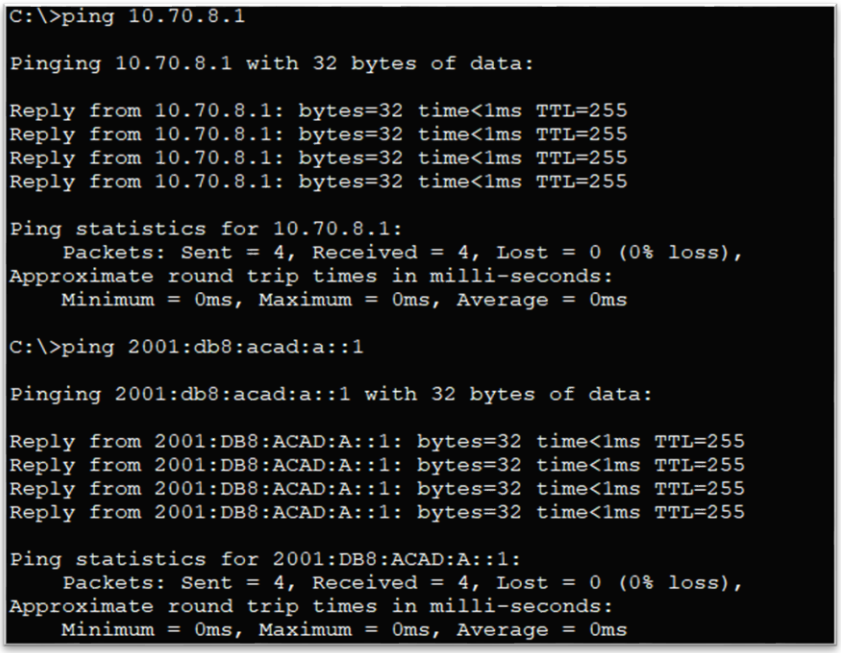
Fuente: Autor

Figura 27: Resultado ping de PC-B a R1 Bucle 0 IPv4 e IPv6



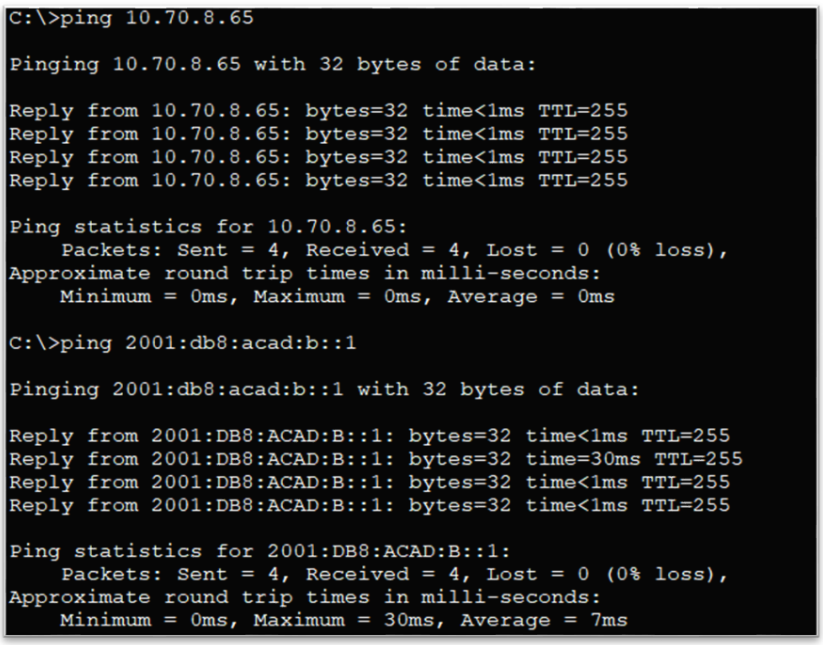
Fuente: Autor

Figura 28: Resultado ping de PC-B a R1, G0/0/1.20 IPv4 e IPv6



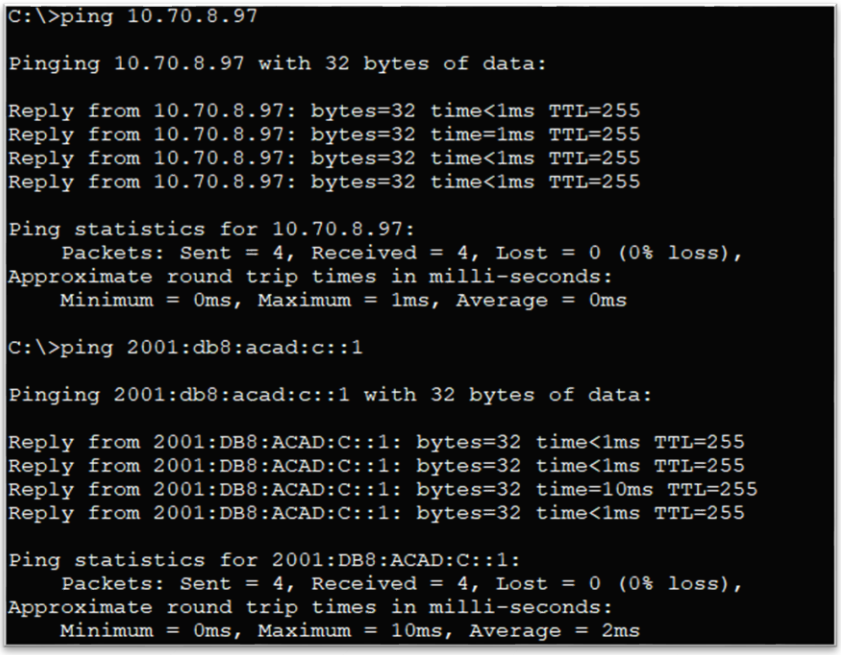
Fuente: Autor

Figura 29: Resultado ping de PC-B a R1, G0/0/1.30 IPv4 e IPv6



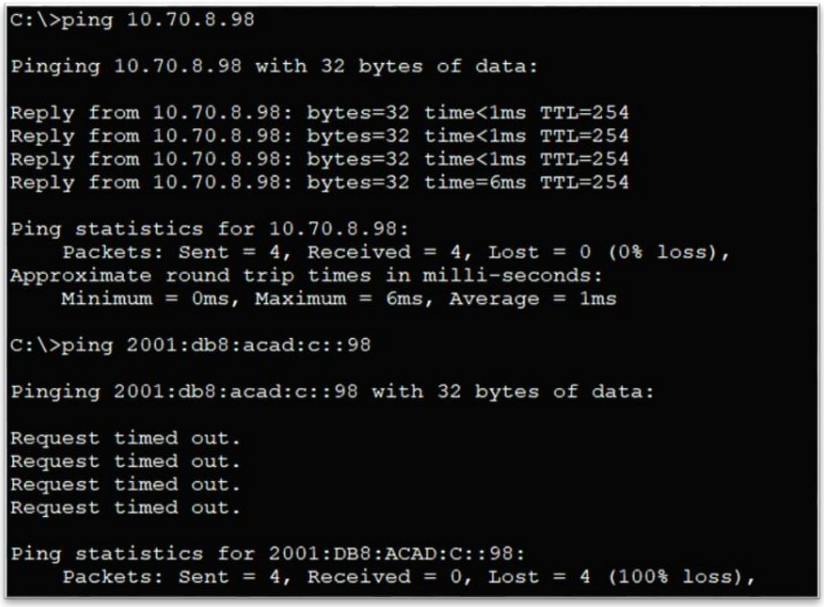
Autor: Fuente

Figura 30: Resultado ping de PC-B a R1, G0/0/1.40 IPv4 e IPv6



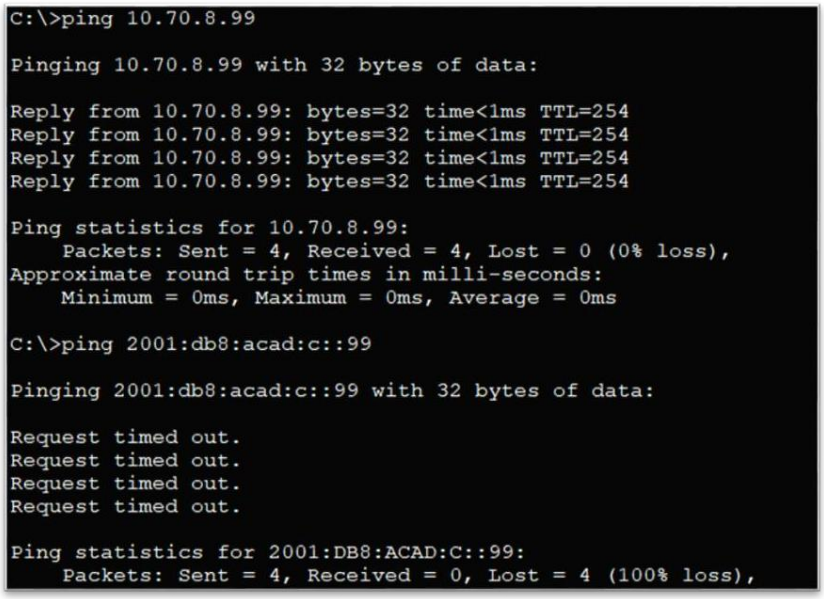
Autor: Fuente

Figura 31: Resultado ping de PC-B a S1, VLAN 40 IPv4 e IPv6



Fuente: Autor

Figura 32: Resultado ping de PC-B a S2, VLAN 40 IPv4 e IPv6



CONCLUSIONES

El escenario 1 nos ayudo a afianzar algunos conceptos básicos pero importantes en la configuración de una red pequeña, aspectos como el desarrollo del direccionamiento IP mediante el proceso del subnetting que se realiza a nivel local, utilizando un rango de direcciones IP privado que podremos utilizar sin limitaciones.

En el escenario 2 encontramos que el switch 2960 no nos permitía configurar la plantilla sdm para que aceptara las configuraciones IPv4 e IPv6, pero esto no fue impedimento ya que solo habilitamos el modo de default bios el cual también nos permitió la habilitación de estos dos protocolos, también encontramos que este switch no nos dejaba ejecutar la función de encapsulation dot1q el cual sustituimos por el comando switchport trunk allowed el cual nos permite especificar el acceso a las VLAN’s que sean necesarias.

Como conclusión general podemos decir que el ir implementando de manera practica los conocimientos adquiridos a la par de la parte teórica fortalece nuestras falencias y nos prepara para enfrentarnos a situaciones reales en nuestra vida profesional.

BIBLIOGRAFIA

CISCO. “Protocolos y comunicaciones de red. Fundamentos de Networking”. {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. “Capa de red. Fundamentos de Networking”. {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. “División de redesIP en subredes. Fundamentos de Networking”. {En línea}. (2019). {25 Noviembre de 2020}.Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. “Redes Conmutadas. Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. “VLAN Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. “Listas de Control de Acceso. Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. “DHCP Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. “NAT para IPv4. Principios de Enrutamiento y Conmutación”. {En línea}. (2019). {27 Noviembre de 2020}.Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

UNAD. “Configuración de Switches y Routers [OVA]”. {En línea}. (2017). {25 Noviembre de 2020}. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD. “Principios de Enrutamiento [OVA]. {En línea}”. (2017). {25 Noviembre de 2020}. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

VESGA, J. Diseño y configuración de redes con Packet Tracer [OVA]. {En línea}. (2014). {25 Noviembre de 2020}. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

ANEXOS

ANEXO A

Enlace de descarga de archivos de simulación: https://drive.google.com/drive/folders/1dGAJGVnWbUE3OdV4B5MaMHxpoxl2v-eA?usp=sharing