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

EYMER GENARO PÁEZ RODRÍGUEZ

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

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

EYMER GENARO PÁEZ RODRÍGUEZ

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

Director
PAULITA FLOR SALAZAR

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

BOGOTÁ, 5 de Diciembre de 2022

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Subneteo: División de una red en redes más pequeñas para facilitar su administración. Es posible optimizar el uso de direcciones de red haciendo uso de VLSM que permite la división de una red en subredes con máscara de subred de longitud variable.[1]

Multiplexado: Combinación de dos o más señales para ser enviadas por un mismo medio de transmisión.

VLAN: LAN Virtual, permite dividir una red en varias redes virtuales que funcionan de forma simultánea en la misma infraestructura física, dividiendo el dominio de difusión y permitiendo aislar y controlar el tráfico entre diferentes VLAN, de esta manera se facilita la administración y el aseguramiento de la red.[2]

Vulnerabilidad: La vulnerabilidad es el grado de debilidad en una red o un dispositivo. La capa de enlace del modelo OSI es la más vulnerable, por lo tanto, es necesario tomar medidas para asegurar una red y así mitigar las amenazas de seguridad de la red.[3]

[1] CISCO NETWORKING ACADEMY, Conceptos de Ethernet. (2022)
[2] CISCO NETWORKING ACADEMY, Conceptos de seguridad LAN. (2022)
[3] CISCO NETWORKING ACADEMY, Comunicación de aplicaciones de red. (2022)

RESUMEN

En el siguiente documento se desarrollan los dos escenarios propuestos como casos de estudio dentro del diplomado de opción de grado del programa de Ingeniería de Sistemas, para ser solucionados haciendo uso de tecnología Cisco. A través de los dos escenarios se podrá verificar el conocimiento adquirido y consolidar las habilidades prácticas requeridas para satisfacer las necesidades del mercado y la sociedad, de ingenieros capacitados en la planeación, diseño, implementación, administración y optimización de redes de telecomunicaciones; habilidades que emergen de la teoría y práctica realizadas durante el diplomado de profundización.

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

ABSTRACT

The following document contains the two scenarios proposed as case studies within the degree option of Systems Engineering program, to be solved using Cisco technology. Through the two scenarios, it will be possible to verify the knowledge acquired and consolidate the practical skills required to satisfy the needs of the market and society, of engineers trained in the planning, design, implementation, administration and optimization of telecommunications networks; skills that emerge from the theory and practice carried out during the course.

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

INTRODUCCIÓN

Este diplomado fortalece el conocimiento impartido durante el programada de Ingeniería de Sistemas sobre redes de telecomunicaciones y telemática. Se abordan los modelos y estándares de mayor uso en la industria, profundizando en el modelo TCP/IP, direccionamiento IPv4 e IPv6, enrutamiento estático y dinámico, mitigación de amenazas de seguridad, diagnóstico y resolución de problemas. Haciendo uso de la tecnología Cisco y buenas prácticas para el diseño e implementación de redes de telecomunicaciones que sean escalables, confiables y seguras.

En el primer escenario se realiza el proceso de división en subredes con máscara de subred variable para dar cumplimiento a los requisitos de cada subred: LAN1 con capacidad para 60 host y LAN2 con capacidad para 20 host. En este primer escenario se configura el direccionamiento IPv4 en los dispositivos, incluida la interfaz SVI para administración remota del switch. Se realizan las configuraciones básicas de seguridad y cifrado de credenciales para el modo Usuario y modo Privilegiado, para acceso a los dispositivos intermedios a través de consola y líneas VTY, para estas últimas se crean llaves RSA y se especifica SSH como el tipo de tráfico permitido para las conexiones remotas.

El segundo escenario se configuran redes LAN Virtuales, que permiten la creación de varias redes lógicas que coexisten en una misma red física, se aplican aspectos de seguridad adicionales en los puertos del switch, enrutamiento estático IPv4 e IPv6, configuración de servicios DHCPv4 y DHCPv6, enrutamiento entre VLAN y conceptos adicionales de conmutación y del Protocolo de Árbol de Expansión STP. Se configura la seguridad similar a la descrita para el primer escenario y se agrega seguridad adicional en los puertos de los switches para proteger la red de vulnerabilidades como saltos y doble etiquetado de VLAN, agotamiento y suplantación de DHCP, suplantación y envenenamiento ARP y ataques de BPDU.

DESARROLLO DE ESCENARIO 1

Aspectos básicos/situación

En el desarrollo del caso de estudio se implementa la topología mostrada en la figura y se configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada se realiza el subnetting y para cumplir el requerimiento para la LAN1 (60 host) y la LAN2 (20 hosts)

Figura 1. Escenario 1

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Figura 2. Simulación de escenario 1

Fuente: Autoría propia.

La figura anterior muestra la simulación en la herramienta de Packet tracer, se observa la topología y conexión física de la red propuesta en el escenario 1, se incluye la conexión por consola a los dispositivos intermedios para su posterior configuración.

Esquema de direccionamiento IP, para LAN1(60 host) y LAN2 (20 hosts): Red inicial 172.**60**.3.0/24. Se inicia dividiendo la red inicial 172.**60**.3.0/24 en 4 redes de 64 host (62 disponibles para asignar a dispositivos), para cumplir con el requisito de LAN1 (60 host). Luego se divide la red segunda red obtenida en el paso anterior **172.60.3.64/26**, en dos redes de 32 host (30 disponibles para asignar a dispositivos) cumpliendo con el requisito de LAN2 (20 host). Se usan las subredes 172.60.3.0/26 para LAN1(60 host) y la red 172.60.3.64/27 para LAN2(20 host).

Tabla 1. Proceso de obtención de subredes Escenario 1

Red inicial	172.60.3.0 /24	11111111 255	11111111 255	11111111 255	00000000 00000000
Redes para 50 host (64)	172.60.3.0 /26	11111111 255	11111111 255	11111111 255	11000000 192
	172.60.3.64 /26	11111111 255	11111111 255	11111111 255	11000000 192
	172.60.3.128 /26	11111111 255	11111111 255	11111111 255	11000000 192
	172.60.3.192 /26	11111111 255	11111111 255	11111111 255	11000000 192
Subred inicial	172.60.3.64 /26	11111111 255	11111111 255	11111111 255	11000000 192
Redes para 25 host (32)	172.60.3.64 /27	11111111 255	11111111 255	11111111 255	11100000 224
	172.60.3.96 /27	11111111 255	11111111 255	11111111 255	11100000 224

Fuente: Autoría propia.

Tabla 2. Detalle de subredes seleccionadas para la configuración

IP de red	**172.60.3.0**
Primera dirección de host	172.60.3.1
Última dirección de host	172.60.3.62
IP broadcast	172.60.3.63
IP de red	**172.60.3.64**
Primera dirección de host	172.60.3.65
Última dirección de host	172.60.3.94
IP broadcast	172.60.3.95

Fuente: Autoría propia.

Tabla 3. Esquema de direccionamiento

Ítem	Requerimiento
Dirección de Red	172.**60**.3.0
Requerimiento de hostSubred LAN1	60
Requerimiento de hostSubred LAN2	20
R1 G0/0/1	172.60.3.62
R1 G0/0/0	172.60.3.94
S1 SVI	172.60.3.2
PC-A	172.60.3.10
PC-B	172.60.3.74

Fuente: Autoría propia.

Configuración de aspectos básicos

Configuración para R1 incluyen las siguientes tareas:

Desactivar la búsqueda DNS

Se desactiva la búsqueda de servidor de nombre de dominio

Router(config)#no ip domain-lookup

Nombre del router R1

Router(config)#hostname R1

Nombre de dominio ccna-sa.com

R1(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado ciscoenpass

Se realiza el cifrado, usando "secret", por defecto usa cifrado MD5

R1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola ciscoconpass

Se ingresa a la línea de consola y para configurar la contraseña, se habilita el servicio de login

R1(config)#line console 0

R1(config-line)#password ciscoconpass

R1(config-line)#login

Establecer la longitud mínima para las contraseñas 10

R1(config)#security password min-length 10

Crear un usuario administrativo en la base de datos local (user: **admin** clave: **admin1pass**)

*Con este comando se crea un usuario **admin** con privilegio 15 (administrador), con una clave encriptada con MD5, lo cual se especifica con el valor **0***

R1(config)#username *admin* privilege 15 secret 0 *admin1pass*

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

Se ingresa a las líneas VTY y se configura login con la base de datos local

R1(config)#line vty 0 4

R1(config-line)#login local

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

Se define el tipo de tráfico que va a aceptar por líneas VTY

R1(config-line)#transport input ssh

Cifrar las contraseñas de texto no cifrado

Servicio que permite encriptar las contraseñas de texto

R1(config)#service password-encryption

Configurar un banner MOTD

Se configura el mensaje del día (MOTD) con los valores datos solicitados

R1(config)#banner motd # Acceso a R1 restringido a personal autorizado! Eymer Genaro Paez Rodriguez - Ingenieria de Sistemas - Diplomado de profundizacion CCNA - Grupo 21 #

Establecer la descripción, establecer la dirección IPv4, activar la interfaz:

Se ingresa a la interfaz correspondiente, se configura la descripción y la dirección IP con su correspondiente máscara de subred

Configuración de interface G0/0/0

R1(config)#interface gi0/0/0

R1(config-if)#description #Puerta de enlace LAN2#

R1(config-if)#ip address 172.60.3.94 255.255.255.224

R1(config-if)#no shutdown

Configuración de interface G0/0/1

R1(config)#interface gi0/0/1

R1(config-if)#description #Puerta de enlace LAN1#

R1(config-if)#ip address 172.60.3.62 255.255.255.192

R1(config-if)#no shutdown

Generar una clave de cifrado RSA Módulo de 1024 bits

Con este comando se genera una clave para cifrar el tráfico del router, se debe indicar los bits, en este caso 1024 que es el tamaño recomendado. Al ejecutar el comando la salida confirma que la clave RSA ha sido creada.

R1(config)#crypto key generate rsa general-keys 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]

Configuración de S1 incluye lo siguiente:

Desactivar la búsqueda DNS

Se desactiva la búsqueda de servidor de nombre de dominio

Switch(config)#no ip domain-lookup

Nombre del switch S1

Switch(config)#hostname S1

Nombre de dominio ccna-sa.com

S1(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado ciscoenpass

El parámetro Secret permite crear una contraseña cifrada en formato MD5

S1(config)#enable secret ciscoenpass

Contraseña de acceso a la consola ciscoconpass

S1(config)#line console 0

S1(config-line)#password ciscoconpass

S1(config-line)#login

Apagar todos los puertos sin usar F0/1-4, F0/7-24, G0/1-2

S1(config)#interface range F0/1-4, F0/7-24, G0/1-2

S1(config-if-range)#shutdown

Se ejecuta el comando para ingresar al rango de interfaces y desactivarles, pero posteriormente se habilita la interfaz G0/1 que se usa para la comunicación con el router R1

S1(config)#interface gi0/1

S1(config-if)#no shutdown

Crear un usuario administrativo en la base de datos local (User: admin Contraseña: admin1pass)

S1(config)#username admin privilege 15 secret 0 admin1pass

Configure el inicio de sesión en las líneas VTY para que use la base de datos local

S1(config)#line vty 0 4

S1(config-line)#login local

Configurar las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line)#transport input ssh

Cifrar las contraseñas de texto no cifrado

S1(config)#service password-encryption

Configurar un banner MOTD

S1(config)#banner motd # Acceso a S1 restringido a personal autorizado! Eymer Genaro Paez Rodriguez - Ingenieria de Sistemas - Diplomado de profundizacion CCNA - Grupo 21 #

Generar una clave de cifrado RSA Módulo de 1024 bits

S1(config)#crypto key generate rsa general-keys 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]

Configurar la interfaz de administración (SVI) en VLAN1. Establecer la descripción y establecer la dirección IPv4

S1(config)#interface vlan1
S1(config-if)#description #Interfaz de administracion de S1#
S1(config-if)#ip address 172.60.3.2 255.255.255.192
S1(config-if)#no shutdown

Se configura la puerta de enlace por defecto para el Switch R1, esta será la IP configurada en la interfaz correspondiente en R1.

S1(config)#ip default-gateway 172.60.3.62

Configuración de los equipos

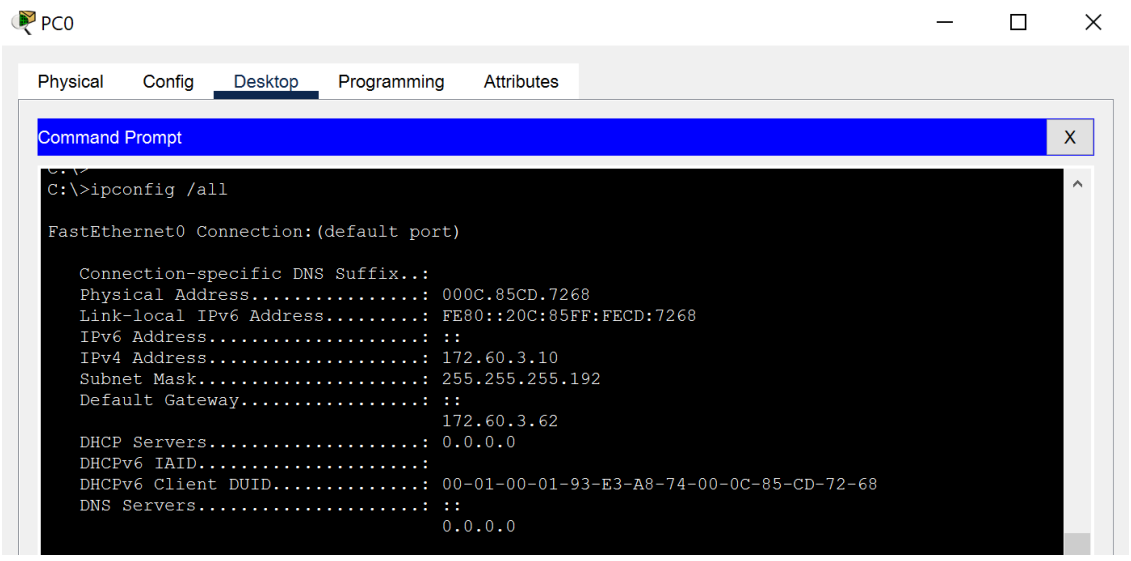
Configuración de los equipos host PC-A y PC-B conforme a la tabla de direccionamiento.

Tabla 4. Configuración solicitada PC-A

Configuración de red de PC-A	
Descripción	PC escritorio LAN1
Dirección física	000C.85CD.7268
Dirección IPv4	172.60.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4predeterminada	172.60.3.62

Fuente: Autoría propia.

Figura 3. Configuración IP PCA



Fuente: Autoría propia.

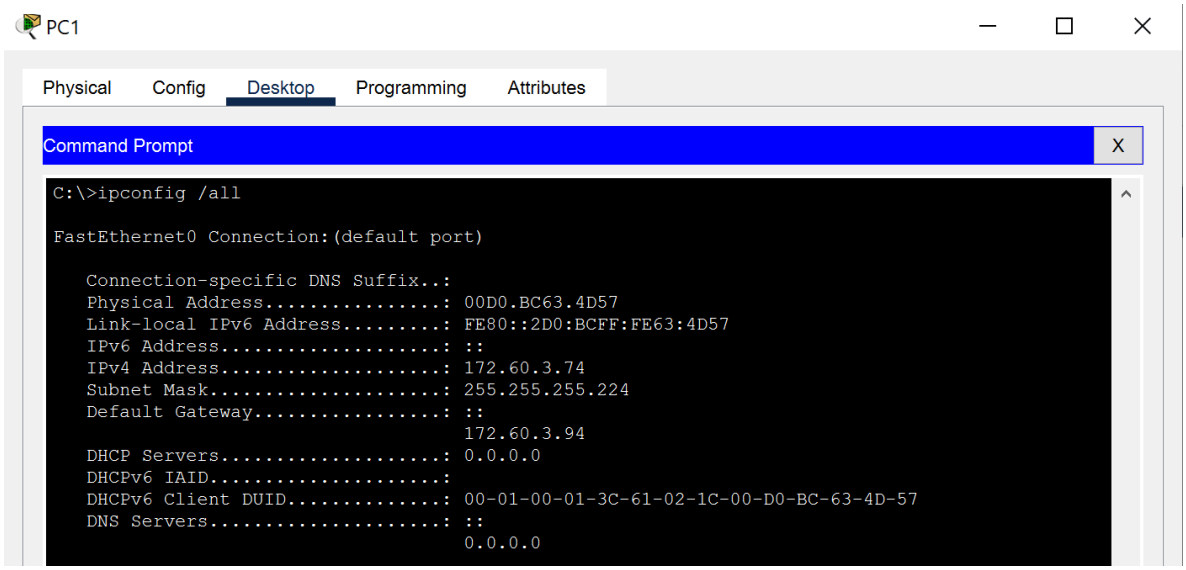
La Figura 3 muestra la configuración IP del PC-A

Tabla 5. Configuración solicitada PC-B

Configuración de red de PC-B	
Descripción	PC escritorio LAN2
Dirección física	00D0.BC63.4D57
Dirección IPv4	172.60.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4predeterminada	172.60.3.94

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Figura 4. Configuración IP PCB



Fuente: Autoría propia.

La Figura 3 muestra la configuración IP del PC-B

Prueba y verificación de la conectividad de extremo a extremo

Se usa la siguiente tabla para registrar la conectividad con cada uno de los dispositivos de red. Se utiliza el comando ping para probar la conectividad entre los dispositivos.

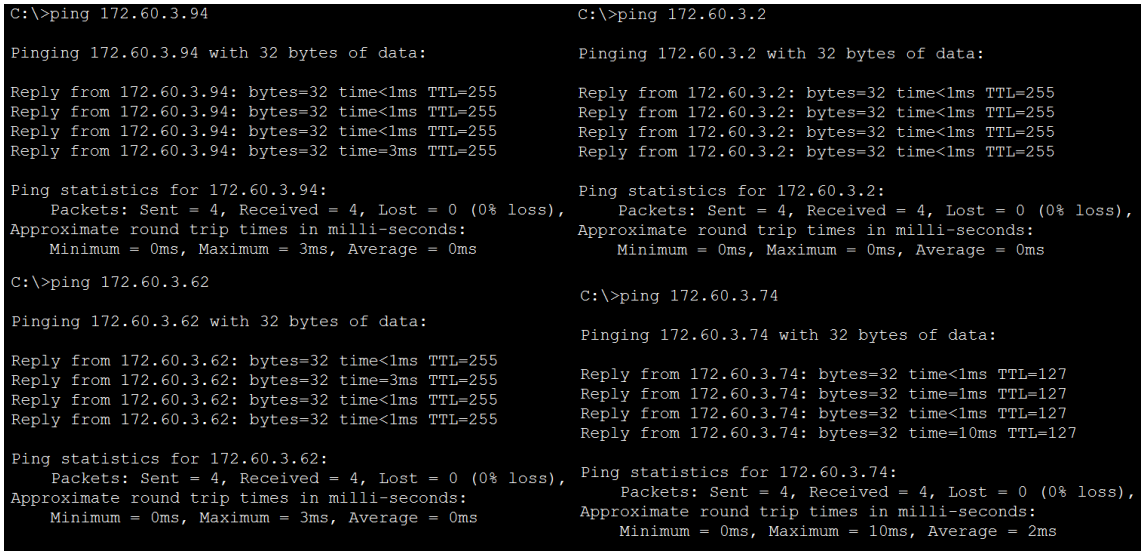
Tabla 6. Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.60.3.94	Exitosa
	R1 G0/0/1	172.60.3.62	Exitosa
	S1 VLAN 1	172.60.3.2	Exitosa
	PC-B	172.60.3.74	Exitosa
PC-B	R1 G0/0/0	172.60.3.94	Exitosa
	R1 G0/0/1	172.60.3.62	Exitosa
	S1 VLAN1	172.60.3.2	Exitosa

Fuente: Autoría propia.

Las pruebas registradas en la tabla anterior se muestran a continuación en la Figura 5 y Figura 6, como se observa a continuación, las pruebas de Ping son exitosas entre los diferentes dispositivos de red:

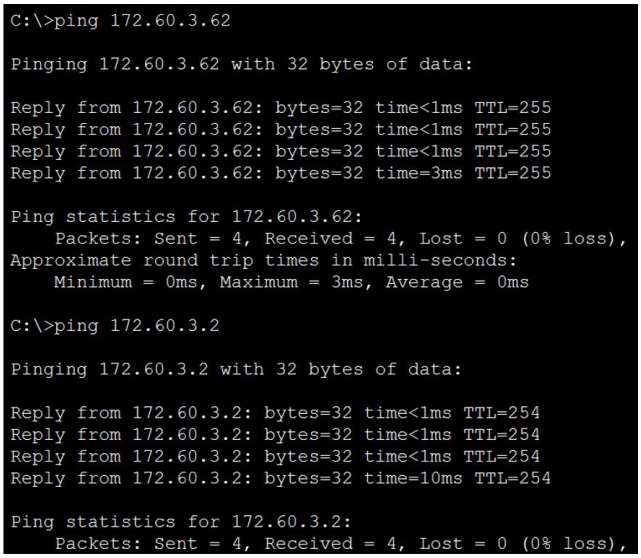
Figura 5. Pruebas de ping desde PC-A



Fuente: Autoría propia.

Ping exitoso desde PC-A hacia interfaces de R1, interfaz SVI de switch S1 y PC-B.

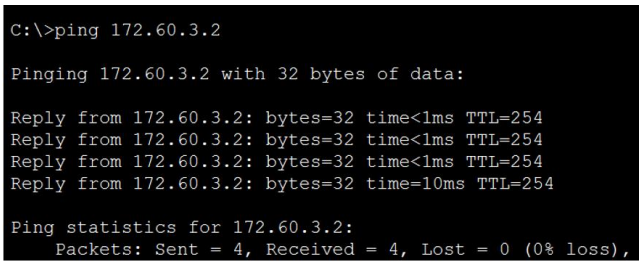
Figura 6. Pruebas de ping desde PC-B



Fuente: Autoría propia.

Pruebas de ping exitosas desde PC-B hacia router R1 y SVI de switch S1

Figura 7. Pruebas de ping desde PC-B hacia PC-A

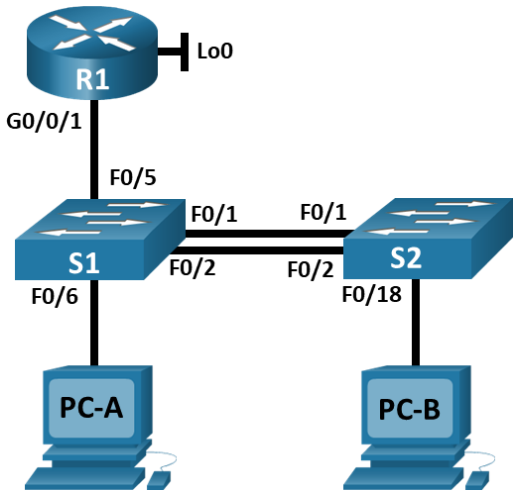


Fuente: Autoría propia.

Pruebas de ping exitosas desde PC-B hacia router R1, hacia la interfaz SVI del switch S1 y hacia la dirección IP en la NIC del PC-A.

DESARROLLO DE ESCENARIO 2

Figura 8. Escenario 2



Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

En este escenario se configuran los dispositivos de una red pequeña. Se realiza la configuración de un router y dos switches que admiten tanto la conectividad IPv4 como IPv6. Se configura seguridad de líneas VTY y enrutamiento entre las VLAN, DHCPv4, Etherchannel y port-security.

Tabla 7. VLAN escenario 2

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

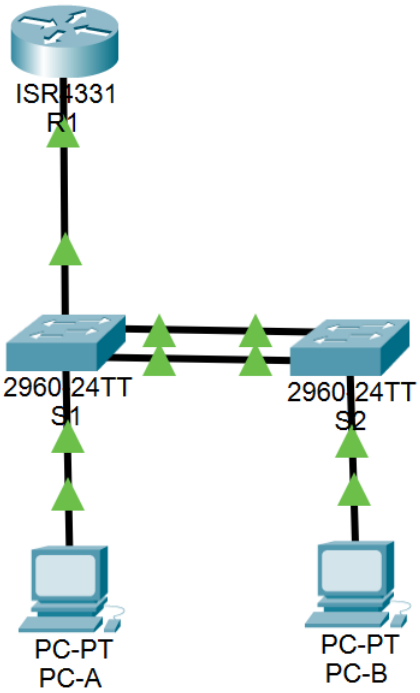
Fuente: Autoría propia.

Tabla 8. Direccionamiento IP

Dispositivo e interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.60.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.60.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.60.8.97 /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	10.60.8.98 /29	10.60.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.60.8.99 /29	10.60.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP paraIPv4	DHCP para puerta de enlace predeterminadaIPv4
	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: Autoría propia.

Figura 9. Simulación del escenario 2



Fuente: Autoría propia.

Parte1: Inicialización, Recarga y Configuración básica de los dispositivos

Switch1

- Se borran de la NVRAM las configuraciones de inicio y archivos VLAN.dat

```
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#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

- Se confirma eliminación de archivos vlan.dat de la memoria flash:

Switch#show flash
Directory of flash:/
1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin
64016384 bytes total (59345929 bytes free)

- Se carga nuevamente el dispositivo.

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...

- Una vez recargado el switch, se configura la plantilla SDM para que admita IPv6 y se vuelve a cargar el dispositivo. Se configura DUAL Stack IPv4 – IPv6

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.

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]

Switch2

- Se borran de la NVRAM las configuraciones de inicio y archivos VLAN.dat

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

- Se confirma eliminación de archivos vlan.dat de la memoria flash:

Switch#show flash
Directory of flash:/
1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin
64016384 bytes total (59345929 bytes free)

- Se carga nuevamente el dispositivo.

```
Switch#reload
Proceed with reload? [confirm]
```

- Una vez recargado el switch, se configura la plantilla SDM para que admita IPv6 y se vuelve a cargar el dispositivo.

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

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

Router 1

- Se borran de la NVRAM las configuraciones de inicio y archivos VLAN.dat

```
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#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

- Se confirma eliminación de archivos vlan.dat de la memoria flash:
  Router#show flash

  System flash directory:
  File Length Name/status
  3 486899872isr4300-universalk9.16.06.04.SPA.bin
  2 28282 sigdef-category.xml
  1 227537 sigdef-default.xml
  [487155691 bytes used, 2761893909 available, 3249049600 total]
  3.17338e+06K bytes of processor board System flash (Read/Write)

- Se carga nuevamente el dispositivo
  Router#reload
  Proceed with reload? [confirm]
  Initializing Hardware ...
  Checking for PCIe device presence...done
  System integrity status: 0x610
  Rom image verified correctly

Paso 2: Configuración de R1

Se realizan las tareas de configuración requeridas en el escenario 2 para el router:

Se desactiva la búsqueda DNS

Router(config)#no ip domain-lookup

Nombre del router - R1

Router(config)#hostname R1

Nombre de dominio - ccna-sa.com

R1(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado - class

Se realiza el cifrado, usando “secret”, por defecto usa cifrado MD5

R1(config)#enable secret class

Contraseña de acceso a la consola – cisco

Se configura contraseña y se habilita login en línea de consola

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

Se establece la longitud mínima para las contraseñas - 5 caracteres

R1(config)#security password min-length 5

Se crea un usuario administrativo en la base de datos local - Nombre de usuario: admin Password: admin1pass. Se configura usuario con privilegios de administrador 15 y clave cifrada con MD5

R1(config)#username admin privilege 15 secret 0 admin1pass

Se configura inicio de sesión en las líneas VTY para usar la base de datos local

R1(config)#line vty 0 4

R1(config-line)#login local

Se configuran líneas VTY para que solo acepten SSH

R1(config-line)#transport input ssh

Se cifran las contraseñas de texto no cifrado

R1(config)#service password-encryption

Se configura un MOTD Banner - Contiene el nombre del dispositivo, el nombre y el programa académico.

Se configura el mensaje del día (MOTD):

R1(config)#banner motd # Acceso a R1 restringido a personal autorizado! Eymer Genaro Paez Rodriguez - Ingenieria de Sistemas - Diplomado de profundizacion CCNA - Grupo 21 #

Se habilita el routing IPv6

R1(config)#ipv6 unicast-routing

Se configura interfaz G0/0/1 y subinterfaces. Se configuran las subinterfaces de acuerdo con la tabla de direccionamiento: Se establece la dirección IPv4, la dirección local de enlace IPv6 como fe80::1, la dirección IPv6 y se activa la interfaz.

G0/0/1.20

R1(config)#interface gi0/0/1.20
R1(config-subif)#description Default Gateway para VLAN 20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.60.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

G0/0/1.30

R1(config-subif)#interface gi0/0/1.30
R1(config-subif)#description Default Gateway para VLAN 30

R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 10.60.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

G0/0/1.40

R1(config-subif)#interface gi0/0/1.40
R1(config-subif)#description Default Gateway para VLAN 40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 10.60.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

G0/0/1.56

R1(config-if)#interface gi0/0/1.56
R1(config-subif)#encapsulation dot1Q 56 native
R1(config-subif)#description Subinterface para VLAN Nativa

Se enciende la interfaz física

R1(config)#interface gi0/0/1
R1(config-if)#no shutdown

Se configura el Loopback0 interface - Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1

R1(config)#interface Loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local

Se genera una clave de cifrado RSA - Módulo de 1024 bits

```
R1(config)#crypto key generate rsa general-keys 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 2 2:32:21.446: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Paso 3: Configuración de S1 Y S2

Se realizan las tareas de configuración requeridas en el escenario 2 para cada switch:

Configuración de S1

Se desactiva la búsqueda DNS.

```
Switch(config)#no ip domain-lookup
```

Nombre del switch - S1 o S2, según proceda

```
Switch(config)#hostname S1
```

Nombre de dominio - ccna-sa.com

```
S1(config)#ip domain-name ccna-sa.com
```

Contraseña cifrada para el modo EXEC privilegiado - class

```
S1(config)#enable secret class
```

Contraseña de acceso a la consola - cisco

```
S1(config)#line console 0
```

S1(config-line)#password cisco
S1(config-line)#login

Se crea un usuario administrativo en la base de datos local - Nombre de usuario: admin Password: admin1pass

S1(config)#username admin privilege 15 secret 0 admin1pass

Se configura el inicio de sesión en las líneas VTY para use la base de datos local

S1(config)#line vty 0 4
S1(config-line)#login local

Se configura las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line)#transport input ssh

Se cifran las contraseñas de texto no cifrado

S1(config-line)#password service-encryption

Se configura un MOTD Banner - Contiene el nombre del dispositivo, el nombre y el programa académico.

S1(config)#banner motd # Acceso a R1 restringido a personal autorizado! Eymer Genaro Paez Rodriguez - Ingenieria de Sistemas - Diplomado de profundizacion CCNA - Grupo 21 #

Se genera una clave de cifrado RSA - Módulo de 1024 bits

S1(config)#crypto key generate rsa general-keys 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 5:43:6.122: %SSH-5-ENABLED: SSH 1.99 has been enabled

Se configura la interfaz de administración (SVI) - Establecer la dirección IPv4 de capa 3

Se solicita usar la VLAN 40 (Invitados). La descripción de la misma se agregará en el siguiente apartado de configuración de los switch.

```
S1(config)#interface vlan 40
S1(config-if)#ip address 10.60.8.98 255.255.255.248
```

Se establece la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2

```
S1(config-if)#ipv6 address fe80::98 link-local
```

Se establece la dirección IPv6 de capa 3

```
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
```

Se configura la puerta de enlace predeterminada como 10.60.8.97 para IPv4

```
S1(config-if)#ip default-gateway 10.60.8.97
```

Configuración de S2

Se desactiva la búsqueda DNS.

```
Switch(config)#no ip domain-lookup
```

Nombre del switch - S1 o S2, según proceda

```
Switch(config)#hostname S2
S2(config)#
```

Nombre de dominio - ccna-sa.com

S2(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado - class

S2(config)#enable secret class

Contraseña de acceso a la consola - cisco

S2(config)#line console 0

S2(config-line)#password cisco

S2(config-line)#login

Se crea un usuario administrativo en la base de datos local - Nombre de usuario: admin Password: admin1pass

S2(config)#username admin privilege 15 secret 0 admin1pass

Se configura el inicio de sesión en las líneas VTY para que use la base de datos local

S2(config)#line vty 0 4

S2(config-line)#login local

Se configuran las líneas VTY para que acepten únicamente las conexiones SSH

S2(config-line)#transport input ssh

Se cifran las contraseñas de texto no cifrado

S2(config-line)#service password-encryption

Se configura un MOTD Banner - Contiene el nombre del dispositivo, el nombre y el programa académico.

S2(config)#banner motd # Acceso a R1 restringido a personal autorizado! Eymer Genaro Paez Rodriguez - Ingenieria de Sistemas - Diplomado de profundizacion CCNA - Grupo 21 #

Se genera una clave de cifrado RSA - Módulo de 1024 bits

```
S2(config)#crypto key generate rsa general-keys 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 0:11:0.328: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Se configura la interfaz de administración (SVI) – Se establece la dirección IPv4 de capa 3

```
S2(config)#interface vlan 40
S2(config-if)#ip address 10.60.8.99 255.255.255.248
```

Se establece la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2

```
S2(config-if)#ipv6 address FE80::99 link-local
```

Se establece la dirección IPv6 de capa 3

```
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
```

Se configura la puerta de enlace predeterminada como 10.60.8.97 para IPv4

```
S2(config-if)#ip default-gateway 10.60.8.97
```

Parte 2:

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

Paso 4: Configuración S1

La configuración de S1 incluye las siguientes tareas:

Crear VLAN:

VLAN 20 – Docentes

VLAN 30 – Estudiantes

VLAN 40 – Invitados

VLAN 50 – Usuarios

VLAN 56 - Native

```
S1(config)#vlan 20
S1(config-vlan)#name Docentes

S1(config)#vlan 30
S1(config-vlan)#name Estudiantes

S1(config-vlan)#vlan 40
S1(config-vlan)#name Invitados
%LINK-5-CHANGED: Interface Vlan40, changed state to up

S1(config-vlan)#vlan 50
S1(config-vlan)#name Usuarios

S1(config-vlan)#vlan 56
S1(config-vlan)#name Native
```

Se confirma creación de las VLAN en S1

S1#show vlan:

20 Docentes active

30 Estudiantes active

40 Invitados active

50 Usuarios active

56 Native active

Se crean las troncales 802.1Q para que utilicen la VLAN 56 nativa - Interfaces F0/1, F0/2 y F0/5. Se configuran las interfaces y se desactiva la negociación

F0/1

S1(config)#interface F0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
S1(config-if)#switchport trunk native vlan 56

F0/2

S1(config)#interface F0/2
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
S1(config-if)#switchport trunk native vlan 56

F0/5

S1(config)#interface F0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport nonegotiate
S1(config-if)#switchport trunk native vlan 56

El comando **switchport trunk encapsulation dot1Q** no se requiere en el switch 2960 ya que solamente usa el estándar IEEE 802.1Q, el cual se usa de forma predeterminada en el modo trunk. Como se observa en la salida de los comandos de verificación:

S1#show interface **fa0/1** switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: **trunk**

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: **Off**

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: **56 (Native)**

S1#show interface **fa0/2** switchport

Name: Fa0/2

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: **trunk**

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: **Off**

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: **56 (Native)**

S1#show interface **fa0/5** switchport

Name: Fa0/5

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: **trunk**

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: **Off**

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: **56 (Native**)

Se crea un grupo de puertos EtherChannel que use interfaces F0/1 y F0/2 , se usa el protocolo LACP para la negociación

Se configura el grupo de interfaces en modo LACP **Active**

```
S1(config)#interface range fa0/1-2
S1(config-if-range)#channel-group 1 mode active
```

Se configura modo troncal

```
S1(config)#interface port-channel 1
S1(config-if)#switchport mode trunk
```

Se configuran las VLAN admitidas por el grupo 1, la configuración de las interfaces y el grupo deberá coincidir con el otro extremo del Etherchannel que será configurado en S2.

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

Se configuran el puerto de acceso de host para **VLAN 20 - Interface F0/6**

```
S1(config)#interface fa0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

Se configuran la seguridad del puerto en los puertos de acceso, para permitir 4 direcciones MAC

```
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 4
S1(config-if)#switchport port-security mac-address sticky

S1#sh port-security interface fa0/6
Port Security : Enabled
Port Status : Secure-up
```

Violation Mode : **Shutdown**
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 4
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Se protegen todas las interfaces no utilizadas, se asignan a VLAN 50 y se establecen en modo de acceso. Se agrega una descripción y se apagan

```
S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 50
S1(config-if-range)#description SIN USAR
S1(config-if-range)#shutdown
```

Se verifican las interfaces que quedan encendidas:

```
S1#sh ip interface brief | include up
Port-channel1 unassigned YES manual up up
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/5 unassigned YES manual up up
FastEthernet0/6 unassigned YES manual up up
Vlan40              10.60.8.98 YES manual up up
```

Paso 5: Configuración de S2

La configuración de S2 incluye las siguientes tareas:

Se crea VLAN:

VLAN 20 – Docentes

VLAN 30 – Estudiantes

VLAN 40 – Invitados

VLAN 50 – Usuarios

VLAN 56 - Native

```
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config-vlan)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config-vlan)#vlan 40
%LINK-5-CHANGED: Interface Vlan40, changed state to up
S2(config-vlan)#name Invitados
S2(config-vlan)#vlan 50
S2(config-vlan)#name Usuarios
S2(config-vlan)#
S2(config-vlan)#vlan 56
S2(config-vlan)#
S2(config-vlan)#name Native
```

Se confirma la creación de las VLAN en S2

```
S2#show vlan brief
20 Docentes active
30 Estudiantes active
40 Invitados active
50 Usuarios active
56 Native active
```

Se crean troncales 802.1Q que utilicen la VLAN 56 nativa - Interfaces F0/1, F0/2. Se configuran las interfaces y se desactiva la negociación

```
S2(config)#interface f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport nonegotiate
S2(config-if)#switchport trunk native vlan 56
```

```
S2(config-if)#interface f0/2
S2(config-if)#switchport mode trunk
S2(config-if)#switchport nonegotiate
S2(config-if)#switchport trunk native vlan 56
```

El comando **switchport trunk encapsulation dot1Q** no se requiere en el switch 2960 ya que usa por defecto el estándar IEEE 802.1Q, el cual se usa de forma predeterminada en el modo trunk. Como se observa en la salida de los comandos de verificación:

```
S2#show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 56 (Native)
```

S2#show interface fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: **trunk**
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: **Off**
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: **56** (Native)

Se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 - Usar el protocolo LACP para la negociación

Se configura el grupo de interfaces en modo LACP **Active**
S2(config)#interface range fa0/1-2
S2(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

Se configura el grupo de puertos del port-channel modo Troncal
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk

Se configuran en S2 las VLAN permitidas igual al port-channel en S1
S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56

Se configura el puerto de acceso de host para **VLAN 30 - Interface F0/18**
S2(config)#Interface F0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30

Se configura la seguridad del puerto en los puertos de acceso, para permitir 4 direcciones MAC

```
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 4
S2(config-if)#switchport port-security mac-address sticky
```

Se verifica configuración de port-security y modo acceso

```
S2#show port-security interface fa0/18
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type: Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 4
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Se protegen todas las interfaces no utilizadas, se asignan a VLAN 50 y se establecen en modo de acceso. Se agrega una descripción y se apagan

```
S2(config)#interface range f0/3-17, f0/19-24, gi0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#description SIN USAR
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#shutdown
```

Se verifican las interfaces que quedan encendidas:

S2#sh ip interface brief | include up
Port-channel1 unassigned YES manual up up
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/18 unassigned YES manual up up
Vlan40 10.60.8.99 YES manual up up

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Se configura Default Routing: Creación de rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0

Se crean las rutas predeterminadas para que dirijan todo el tráfico de datos IPv4 e IPv6 hacia la interfaz Loopback 0. En este caso no usamos el Gateway o la dirección IP del siguiente salto sino que definimos la interfaz por la que debe salir el tráfico:
R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback 0
R1(config)#ipv6 route ::/0 Loopback 0

Se configura el servicio DHCPv4 para VLAN 20 – Se crea un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Se asigna el nombre de dominio unad-ccna-sa.net y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada:

R1(config)#ip dhcp pool DHCP_VLAN20
R1(dhcp-config)#network 10.60.8.0 255.255.255.192

Se configura el gateway correspondiente a la VLAN20
R1(dhcp-config)#default-router 10.60.8.1
R1(dhcp-config)#domain-name unad-ccna-sa.net

Se excluyen las direcciones excepto las 10 últimas direcciones de host de la subred y además se excluye dirección de Broadcast IPv4 10.60.8.63
R1(config)#ip dhcp excluded-address 10.60.8.1 10.60.8.52
R1(config)#ip dhcp excluded-address 10.60.8.63

Se configura DHCPv4 para VLAN 30 – Se crea un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Se asigna el nombre de dominio unad-ccna-sb.net y se especifica la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

R1(config)#ip dhcp pool DHCP_VLAN30
R1(dhcp-config)#network 10.60.8.64 255.255.255.224

Se configura el gateway correspondiente a la VLAN20
R1(dhcp-config)#default-router 10.60.8.65
R1(dhcp-config)#domain-name unad-ccna-sb.net

Se excluyen las direcciones excepto las 10 últimas direcciones de host de la subred y además se excluye dirección de Broadcast IPv4 10.60.8.95

R1(config)#ip dhcp excluded-address 10.60.8.65 10.60.8.84
R1(config)#ip dhcp excluded-address 10.60.8.95

Paso 2: Configuración de los dispositivos finales

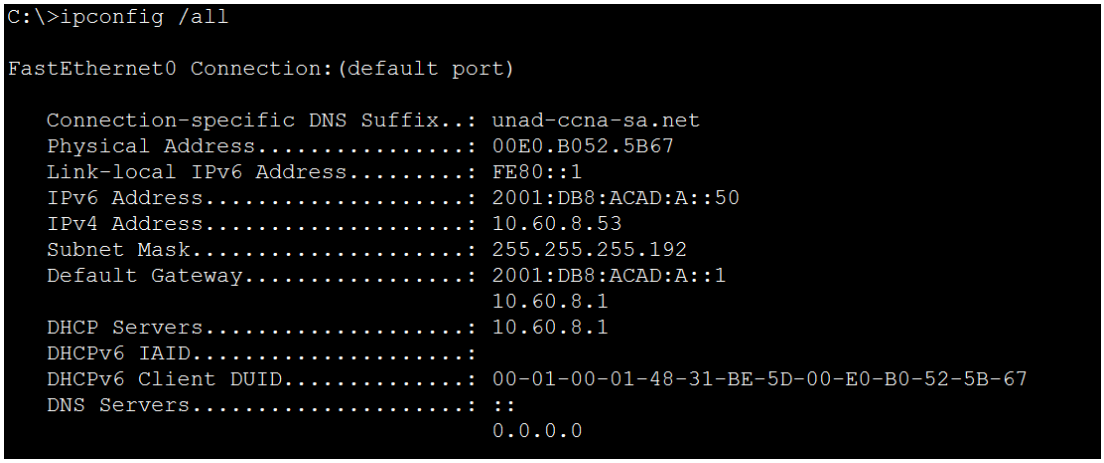
Se configuran los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y se asignan estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor se verifican las configuraciones de red del host con el comando **ipconfig /all**:

Tabla 9. Configuración PC A

Configuración de red de PC-A	
Descripción	Configuración IP cliente vlan20
Dirección física	00E0.B052.5B67
Dirección IP	10.60.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.60.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Figura 10. Configuración IPv4 e IPv6 de PC A



Fuente: Autoría propia.

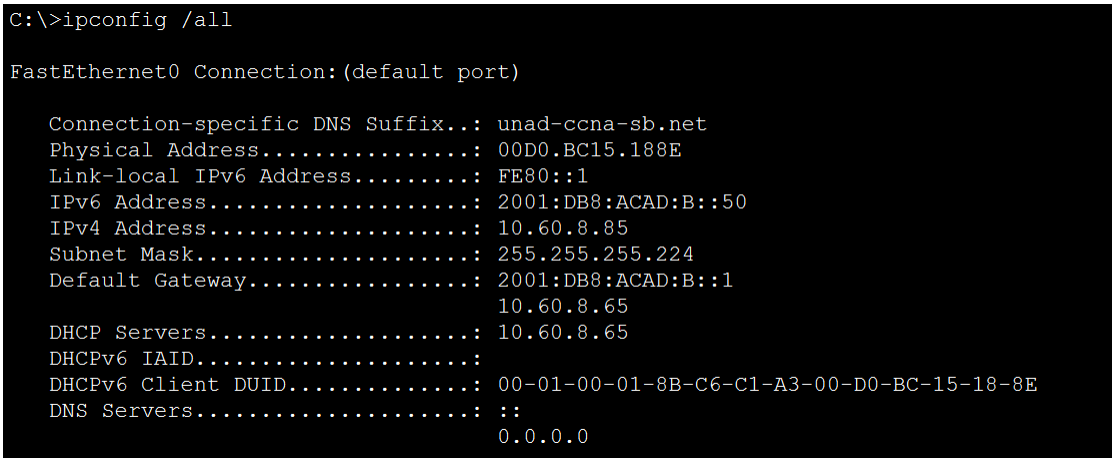
Se confirma el funcionamiento del servicio DHCPv4 del router R1 para PC-A

Tabla 10. Configuración PC B

Configuración de red de PC-A	
Descripción	Configuración IP cliente vlan30
Dirección física	00D0.BC15.188E
Dirección IP	10.60.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.60.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Figura 11. Configuración IPv4 e IPv6 de PC B



Fuente: Autoría propia.

Se confirma el funcionamiento del servicio DHCPv4 del router R1 para PC-B

Parte 3: Probar y verificar la conectividad de extremo a extremo

Se realizan pruebas de conectividad con el comando ping, con resultado exitoso y se registra el resultado en la Tabla 11 para el PC-A y Tabla 12 para PC-B. Se realizan pruebas de Ping para confirmar la conectividad hacia las subinterfaces configuradas en el router para manipular el tráfico asociado a cada una de las VLAN para proporcionar servicio de enrutamiento entre las VLAN, de igual manera se confirma la correcta configuración de las troncales VLAN y el enrutamiento InterVLAN. También se prueba la conectividad hacia las interfaces SVI de los router en las cuales se configura por seguridad una VLAN de administración y una VLAN predeterminada que es diferente a la predeterminada VLAN1.

Tabla 11. Pruebas de conectividad IPv4 e IPv6, Parte 1

Desde	Destino		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.60.8.1	Exitoso
		IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.30	IPv4	10.60.8.65	Exitoso
		IPv6	2001:db8:acad:b::1	Exitoso
	R1, G0/0/1.40	IPv4	10.60.8.97	Exitoso
		IPv6	2001:db8:acad:c::1	Exitoso
	S1, VLAN 40	IPv4	10.60.8.98	Exitoso
		IPv6	2001:db8:acad:c::98	Fallido. Resultado esperado SVI IPv6
	S2, VLAN 40	IPv4	10.60.8.99	Exitoso
		IPv6	2001:db8:acad:c::99	Fallido. Resultado esperado SVI IPv6
	PC-B	IPv4	10.60.8.85	Exitoso
		IPv6	2001:db8:acad:b::50	Exitoso
	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209::1	Exitoso

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Tabla 12. Pruebas de conectividad IPv4 e IPv6, Parte 2

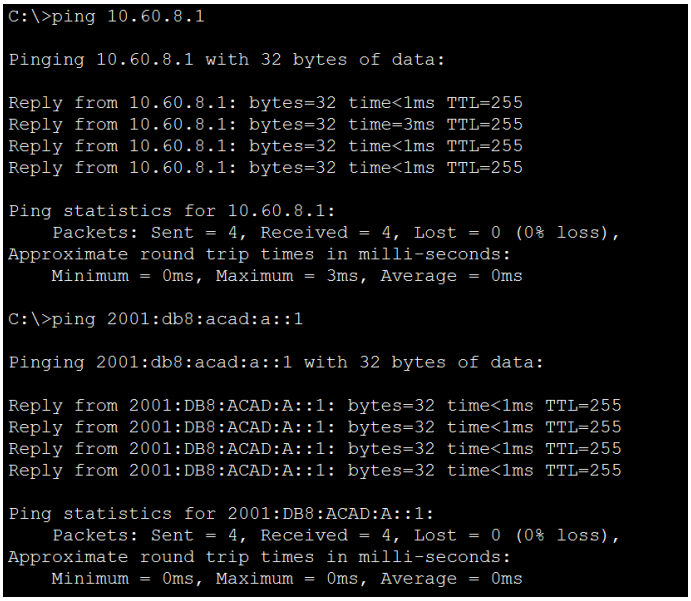
Desde	Destino		Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209::1	Exitoso
	R1, G0/0/1.20	IPv4	10.60.8.1	Exitoso
		IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.30	IPv4	10.60.8.65	Exitoso
		IPv6	2001:db8:acad:b::1	Exitoso
	R1, G0/0/1.40	IPv4	10.60.8.97	Exitoso
		IPv6	2001:db8:acad:c::1	Exitoso
	S1, VLAN 40	IPv4	10.60.8.98	Exitoso
		IPv6	2001:db8:acad:c::98	Fallido. Resultado esperado SVI IPv6
	S2, VLAN 40	IPv4	10.60.8.99	Exitoso
		IPv6	2001:db8:acad:c::99	Fallido. Resultado esperado SVI IPv6

Fuente: Prueba de habilidades práctica, Diplomado de profundización Cisco.

Pruebas de conectividad IPv4 e IPv6

Las pruebas de conectividad son exitosas, excepto las pruebas de Ping IPv6 a la interfaz SVI de los switches, esta prueba fallida es un resultado esperado. Lo anterior se observa en las Figuras 11 a 23, imágenes de las pruebas de Ping a las demás interfaces de los dispositivos son exitosas, confirmándose también el funcionamiento del enrutamiento InterVLAN y las troncales VLAN:

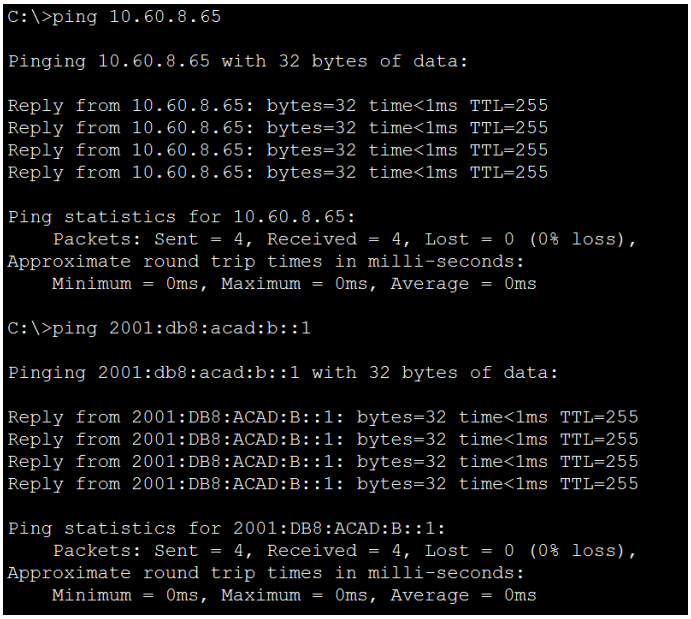
Figura 12. PC-A ping hacia R1, G0/0/1.20



Fuente: Autoría propia.

Ping exitoso desde PC-A hacia la puerta de enlace de la VLAN 20 en el router R1

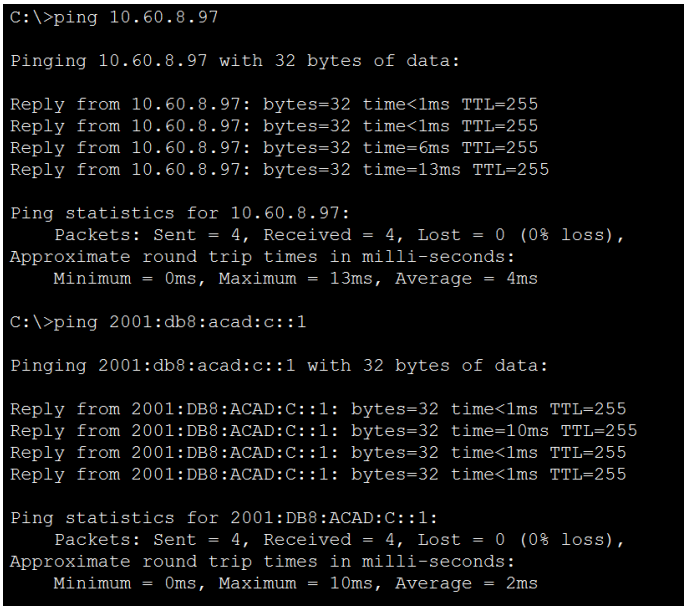
Figura 13. PC-A ping hacia R1, G0/0/1.30



Fuente: Autoría propia.

Ping exitoso desde PC-A hacia la puerta de enlace de la VLAN 30 en el router R1

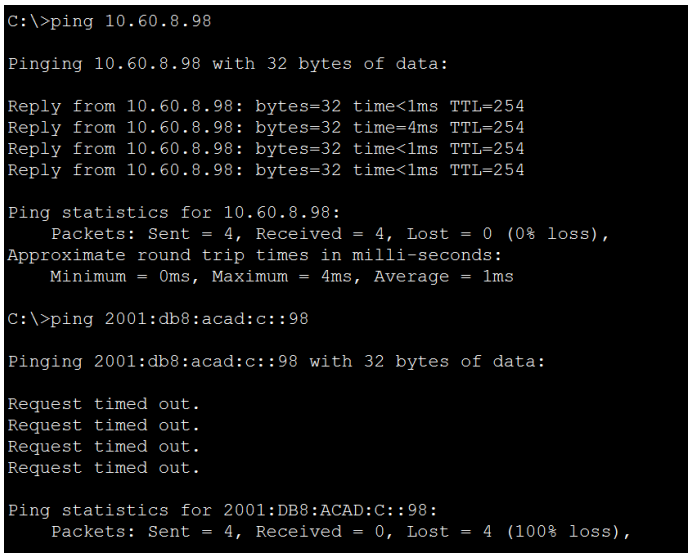
Figura 14. PC-A ping hacia R1, G0/0/1.40



Fuente: Autoría propia.

Ping exitoso desde PC-A hacia la puerta de enlace de la VLAN 40 en el router R1

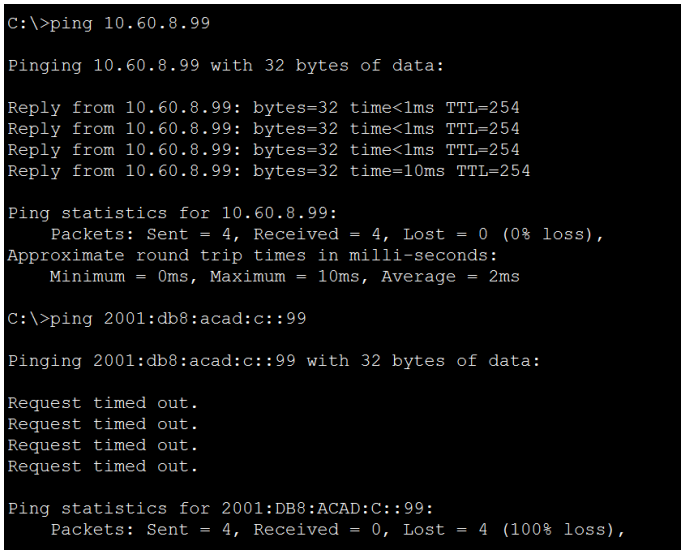
Figura 15. PC-A ping hacia S1, VLAN 40



Fuente: Autoría propia.

Ping IPV4 exitoso desde PC-A hacia la interfaz de administración del switch S1.

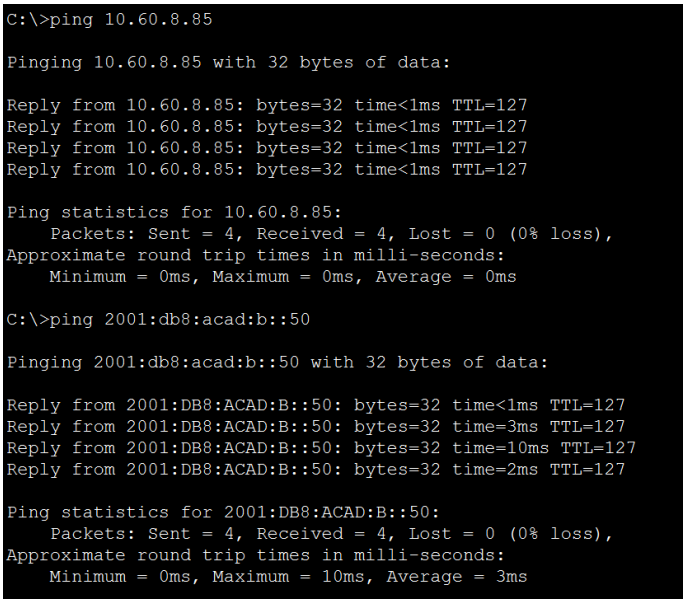
Figura 16. PC-A ping hacia S2, VLAN 40



Fuente: Autoría propia.

Ping IPV4 exitoso desde PC-A hacia la interfaz de administración del switch S2.

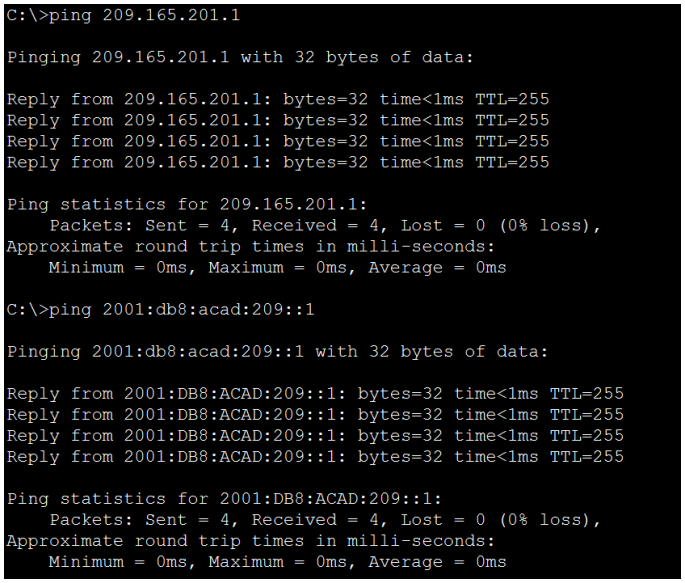
Figura 17. PC-A ping hacia PC-B



Fuente: Autoría propia.

Ping exitoso desde el terminal PC-A hacia el PC-B, confirmando el correcto funcionamiento del enrutamiento InterVLAN.

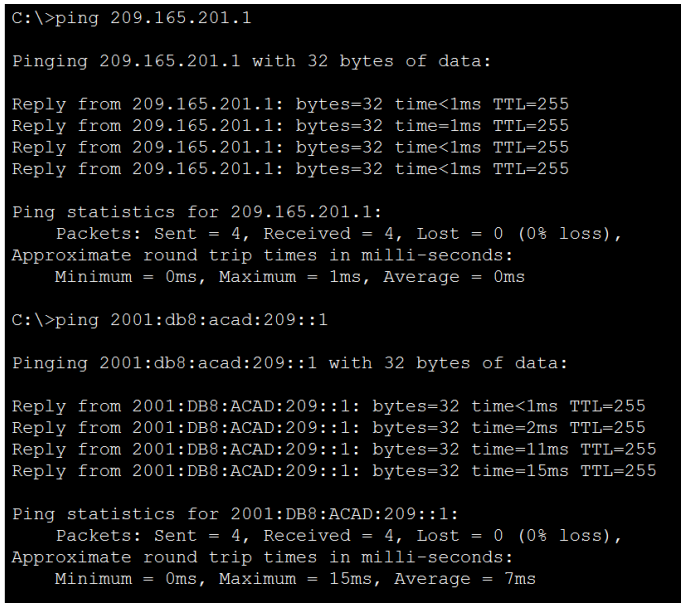
Figura 18. PC-A ping hacia R1 Bucle 0



Fuente: Autoría propia.

Ping exitoso desde PC-A hacia interfaz de bucle invertido Loopback en router R1

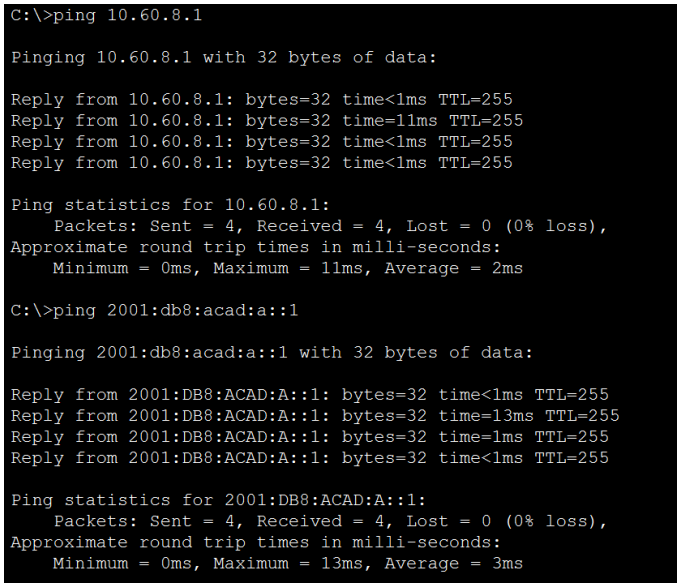
Figura 19. PC-B ping hacia R1 Bucle 0



Fuente: Autoría propia.

Ping exitoso desde PC-B hacia interfaz de bucle invertido Loopback en router R1

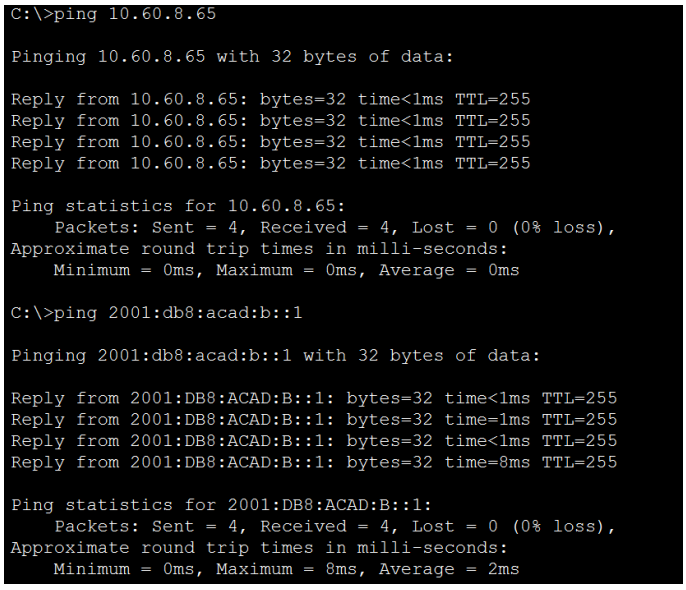
Figura 20. PC-B ping hacia R1, G0/0/1.20



Fuente: Autoría propia.

Ping exitoso desde PC-B hacia la puerta de enlace de la VLAN 20 en router R1

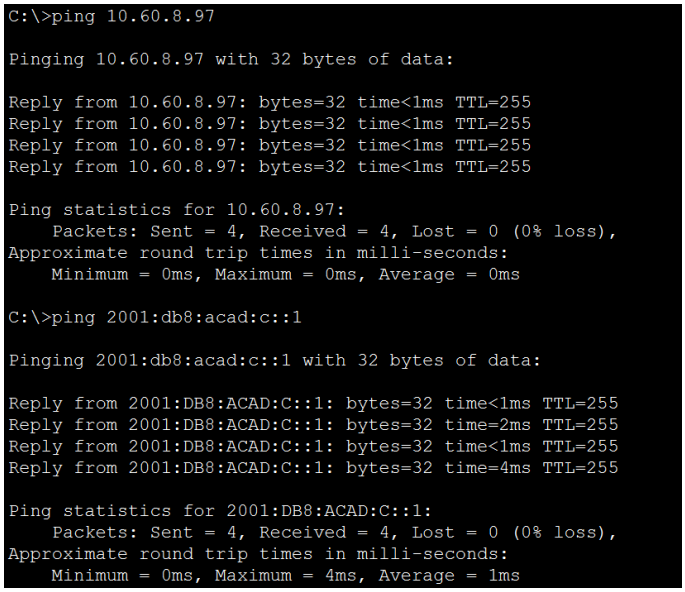
Figura 21. PC-B ping hacia R1, G0/0/1.30



Fuente: Autoría propia.

Ping exitoso desde PC-B hacia la puerta de enlace de la VLAN 30 en router R1

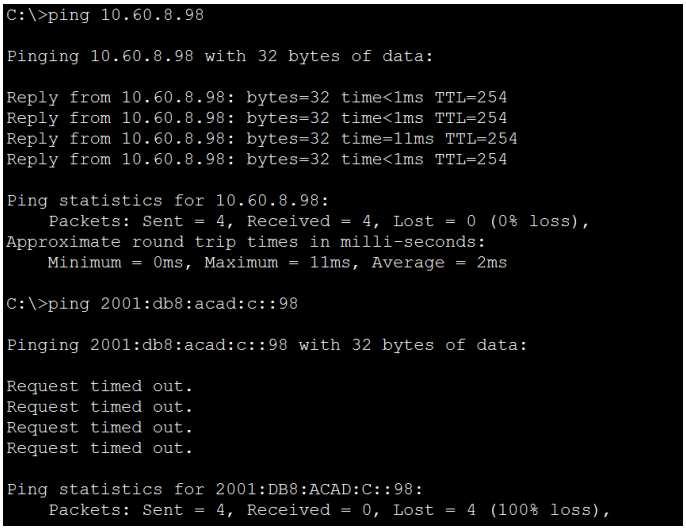
Figura 22. PC-B ping hacia R1, G0/0/1.40



Fuente: Autoría propia.

Ping exitoso desde PC-B hacia la puerta de enlace de la VLAN 40 en router R1

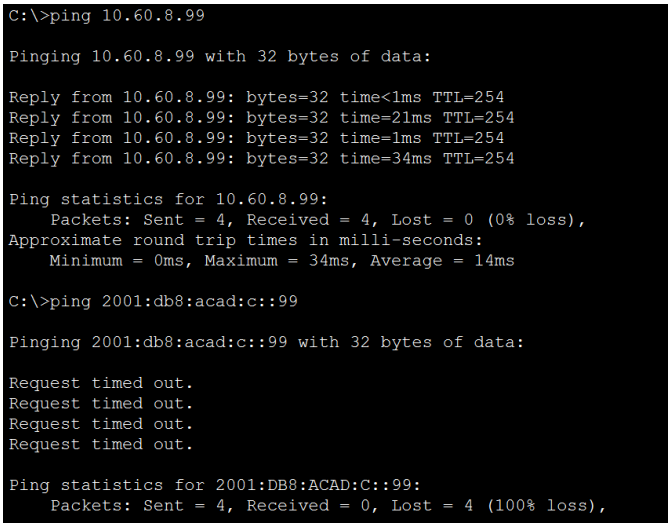
Figura 23. PC-B ping hacia S1, VLAN 40



Fuente: Autoría propia.

Ping IPV4 exitoso desde PC-B hacia la interfaz de administración del switch S1. El ping IPv6 es fallido, un resultado esperado para este escenario.

Figura 24. PC-B ping hacia S2, VLAN 40



Fuente: Autoría propia.

Ping IPV4 exitoso desde PC-B hacia la interfaz de administración del switch S2. El ping IPv6 es fallido, un resultado esperado para este escenario.

CONCLUSIONES

Para diseñar y desplegar una red se deben seleccionar los dispositivos de acuerdo con las prestaciones requeridas y los costos; a nivel de tipo y cantidad de interfaces físicas, seguridad, de sistema operativo IOS, protocolos de red soportados, entre otros. También es importante hacer un uso eficiente de las direcciones IPv4 de host disponibles, para este fin se aplica VLSM para realizar una división en subredes con mascara de subred de longitud variable, de acuerdo con los requerimientos de direcciones de host necesarios para cada subred.

Los dos modelos de uso frecuente que definen y describen el funcionamiento de una red son TCP/IP y OSI, ambos son modelos de capas y se diferencian en cómo se agrupan estas capas. A través de estos modelos se puede describe de forma ordenada y detallada la manera como un mensaje es codificado, empaquetado, segmentado, transmitido, enrutado y entregado al host de destino. En los escenarios se usan dispositivos Router que funcionan en la Capa de Red y dispositivos Switch que funcionan en la Capa de Enlace. Sin embargo, existen los switches multicapa como los Switch Cisco Catalyst que funcionan en capa 2 y capa 3, cumpliendo funciones de conmutación y enrutamiento.

El uso de las LAN Virtuales o VLAN facilita la administración y el aseguramiento de la red, permitiendo dividir la red en diferentes dominios de difusión y aislando el tráfico de determinadas VLAN de acuerdo con las necesidades, de esta manera es posible diseñar e implementar redes LAN seguras teniendo en cuenta las mejores prácticas de seguridad de la capa de enlace. Junto con las VLAN se suele implementar el protocolo de árbol de expansión STP más conocido por su nombre en inglés SpanningTree, cuyas características permiten bloquear interfaces de forma dinámica en un proceso de convergencia que elimina bucles de capa 2. No evitar estos loops eleva el consumo de recursos de red y CPU, afectando el desempeño, llegando incluso a dejar inoperante una red.

BIBLIOGRAFIA

CISCO NETWORKING ACADEMY, Comunicación de aplicaciones de red. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/itn-dl/14.0.1

CISCO NETWORKING ACADEMY, Conceptos de redes Ethernet. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/itn-dl/4.0.1

CISCO NETWORKING ACADEMY, Conceptos de seguridad de LAN. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/srwe-dl/10.0.1

CISCO NETWORKING ACADEMY, Conceptos de STP {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/srwe-dl/5.1.1

CISCO NETWORKING ACADEMY, Conectividad de red básica y comunicaciones. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/itn-dl/1.0.1

CISCO NETWORKING ACADEMY, Crear y asegurar una red pequeña. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/itn-dl/16.0.1

CISCO NETWORKING ACADEMY, Direccionamiento IP. {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://contenthub.netacad.com/itn-dl/8.0.1

TAPIAS, Juan. Introducción a las VLAN [OVI]. Universidad Nacional Abierta y a Distancia {En línea} (2022) {23 Noviembre de 2022} Disponible en: https://repository.unad.edu.co/handle/10596/49452

ANEXOS

Anexo A – Enlace de descarga de los archivos de simulación:

Enlace:
https://drive.google.com/drive/folders/1sbeADWMbpH_Y3DxI5bOi2joqFItaQ49I?usp=sharing