

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

OLGA LUCIA CABALLERO MELGAREJO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUOLA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
BOGOTA
2022

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

OLGA LUCIA CABALLERO MELGAREJO

Diplomado de opción de grado presentado para optar el
Título de INGENIERO DE SISTEMAS

DIRECTOR:
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUOLA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
BOGOTA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C, 22 de noviembre de 2022

AGRADECIMIENTOS

Al realizar este trabajo final como requisito para graduarme, no puedo dejar de sentir que debo agradecer a la Universidad Nacional Abierta y a Distancia U.N.A.D., y por supuesto a las directivas, profesores y hasta compañeros de clase que siempre de diferentes maneras me han ayudado y aportado, cada uno de diferentes maneras, para lograr terminar no solo la carrera de la que hace falta poco ya para culminarla, sino especialmente de este trabajo realizado con mucho esfuerzo y dedicación para optar como requisito de grado.

Siempre tendré presente y aplicaré en mi desarrollo profesional tantas enseñanzas no solo académicas sino personales que me hicieron crecer en ambos aspectos y por cuyos conocimientos estaré eternamente agradecida con todo el personal vinculado de muchas maneras a la Universidad Nacional Abierta y a Distancia U.N.A.D

TABLA DE CONTENIDO

AGRADECIMIENTOS.....	4
TABLA DE CONTENIDO	5
LISTA DE TABLAS	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	12
INTRODUCCIÓN	13
1. ESCENARIO No. 1	14
1.1 CONSTRUCCIÓN DE LA RED.	14
1.3 CONFIGURACIÓN DE ASPECTO BÁSICOS	17
1.4 CONFIGURACIÓN DE LOS EQUIPOS.....	22
1.5 PRUEBA Y VERIFICACIÓN DE LA CONECTIVIDAD DE EXTREMO A EXTREMO	22
2. ESCENARIO NO. 2	29
2.1 CONSTRUCCIÓN DE LA RED	29
2.2 REQUERIMIENTOS.....	29
2.3 CONFIGURACIÓN ASPECTOS BASICOS.....	30
2.4 CONFIGURACIÓN DEL R1.....	34
2.5 CONFIGURACIÓN DEL S1	38
2.6 CONFIGURACIÓN DEL S2.....	40

2.7 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL).....	43
2.8 CONFIGURAR SOPORTE DE HOST	54
2.9 CONFIGURAR LOS SERVIDORES.....	55
2.10 PRUEBAS DE CONECTIVIDAD DE EXTREMO A EXTREMO.....	58
CONCLUSIONES	73
BIBLIOGRAFIA.....	75
ANEXOS.....	76

LISTA DE TABLAS

	pág.
Tabla 1. Requerimientos direccionamiento	14
Tabla 2. Subneteo de redes.....	16
Tabla 3. Direcciones IPv4 de los host.....	16
Tabla 4. (Continuación).....	17
Tabla 5. Configuración PC-A	22
Tabla 6. Configuración PC-B	22
Tabla 7. Resultados pruebas ping	23
Tabla 8. VLAN.....	29
Tabla 9. Asignación de direcciones.....	29
Tabla 10. Configuración de red de PC-A	55
Tabla 11. Configuración de red de PC-B	57
Tabla 12. Resultados de verificación de conexión	59

LISTA DE FIGURAS

	pág.
Figura 1. Topología escenario 1	14
Figura 2. Cálculo máscara red LAN1	15
Figura 3. Cálculo máscara red LAN2	16
Figura 4. Ping desde PC-A a R1 G0/0/0	24
Figura 5. Ping desde PC-A a R1 G0/0/1	24
Figura 6. Ping desde PC-A a S1 VLAN1.....	25
Figura 7. Ping desde PC-A a PC-B.....	25
Figura 8. Ping desde PC-B a R1 G0/0/0	26
Figura 9. Ping desde PC-B a R1 G0/0/1	27
Figura 10. Ping desde PC-B a S1 VLAN1.....	27
Figura 11. Topología escenario 2	29
Figura 12. Configuración por DHCP para PC-A.....	56
Figura 13. Configuración IPv6 de PC-A	56
Figura 14. Configuración por DHCP para PC-B.....	57
Figura 15. Configuración IPv6 de PC-B	58
Figura 16. Verificación de configuración de las PCs.....	58
Figura 17. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.20	60
Figura 18. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.30	61
Figura 19. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.40	62

Figura 20. Verificación comunicación IPv4 e IPv6 desde PC-A a S1 VLAN-40	63
Figura 21. Verificación comunicación IPv4 e IPv6 desde PC-A a S2 VLAN-40	64
Figura 22. Verificación de comunicación PC-A a PC-B	65
Figura 23. Verificación de comunicación de PC-A a R1 Bucle 0.....	66
Figura 24. Verificación de comunicación de PC-B a R1 Bucle 0.....	66
Figura 25. Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.20	68
Figura 26. Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.30	69
Figura 27 Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.40	70
Figura 28. Verificación comunicación IPv4 e IPv6 desde PC-B a S1 VLAN-40	71
Figura 29. Verificación comunicación IPv4 e IPv6 desde PC-B a S2 VLAN-40	72

GLOSARIO

Consola: *“Este es un puerto de administración físico que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de mantenimiento del dispositivo. La ventaja de usar un puerto de consola es que el dispositivo es accesible incluso si no hay servicios de red configurados, como realizar la configuración inicial. Para una conexión de consola se requiere un equipo con software de emulación de terminal y un cable de consola especial para conectarse al dispositivo.”*¹

Dirección física (la dirección MAC): *“Se utiliza para comunicaciones NIC a NIC en la misma red Ethernet.”*²

Dirección lógica (la dirección IP): *“Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino. La dirección IP de destino puede estar en la misma red IP que la de origen o en una red remota.”*³

Hosts: *“El término se refiere específicamente a los dispositivos de la red a los que se asigna un número para fines de comunicación. Este número identifica el host dentro de una red determinada.”*⁴

Internet: Es una colección global de redes interconectadas (internetworks o internet para abreviar). La Internet es como una colección de redes LAN y WAN interconectadas.

Máscara de subred: se usa para identificar la parte de red/host de una dirección IP.

1 CISCO. (2022). *Configuración básica de switches y terminales*. <https://contenthub.netacad.com/itn-dl/2.1.4>

2 CISCO. (2022). *Resolución de dirección*. <https://contenthub.netacad.com/itn-dl/9.1.1>

3 CISCO. (2022). *Resolución de dirección*. <https://contenthub.netacad.com/itn-dl/9.1.1>

4 CISCO. (2022). *Las redes en la actualidad*. <https://contenthub.netaca.com/itn-dl/1.2.1>

RESUMEN

En el siguiente trabajo se simulara la implementación y configuración de dos topologías o escenarios. La simulación se realizara en el software de Packet Tracer de acuerdo a los requerimientos establecidos en la guía.

En el escenario 1 se simulara la configuración de una red pequeña con dos subredes, se utilizaran dispositivos como un router, un switch y dos equipos. Para la configuración de las direcciones IP de las dos subredes se realizara subneteo VLSM de acuerdo a los host requeridos para cada subred. Después se realizara la configuración de requerimientos básicos de los host (nombre, direcciones IP, seguridad, etc.), por último se realizaran pruebas de comunicación.

En el escenario 2 se simula la configuración de una red pequeña, utilizando dispositivos como un router, dos switches y dos equipos. Se realizara la configuración de los dispositivos para que coexistan las configuración de las direcciones IP de los protocolos IPv4 al mismo tiempo con los protocolos de IPv6, así como la configuración de redes VLAN y enlaces troncales de VLAN , por último en este escenario también se realizaran pruebas de comunicación entre las diferentes interfaces.

Palabras Clave: Cisco, Direcciones IP, Dispositivos, Modelo OSI, Protocolos, Redes, Seguridad,

ABSTRACT

In the following work, the implementation and configuration of two topologies or scenarios will be simulated. The simulation will be carried out in the Packet Tracer software according to the requirements established in the guide.

In scenario 1, the configuration of a small network with two subnets will be simulated, devices such as a router, a switch and two computers will be used. For the configuration of the IP addresses of the two subnets, VLSM subnetting will be carried out according to the hosts required for each subnet. Afterwards, the configuration of the basic requirements of the hosts (name, IP addresses, security, etc.) will be carried out, and finally, communication tests will be carried out.

In scenario 2, the configuration of a small network is simulated, using devices such as a router, two switches and two computers. The configuration of the devices will be carried out so that the configuration of the IP addresses of the IPv4 protocols coexist at the same time with the IPv6 protocols, as well as the configuration of VLAN networks and VLAN trunk links, finally in this scenario they will also be carried out communication tests between the different interfaces.

Keywords: Cisco, IP addresses, Devices, OSI Model, Protocols, , Networks, Security,

INTRODUCCIÓN

En este trabajo mediante el software como Packet Tracer se realizara la simulación de dos escenarios de una red LAN y WAN, dando solución a casos típicos de los requerimientos de una empresa; como realizar la configuración de las direcciones IP tanto en IPv4 como IPv6. Para esto es necesario conocer las características tanto de hardware como software de los diferentes dispositivos que se implementaran en la red, el software Packet Tracer permite realizar la verificar las características de estos y poder validar si se da cumplimiento a las necesidades.

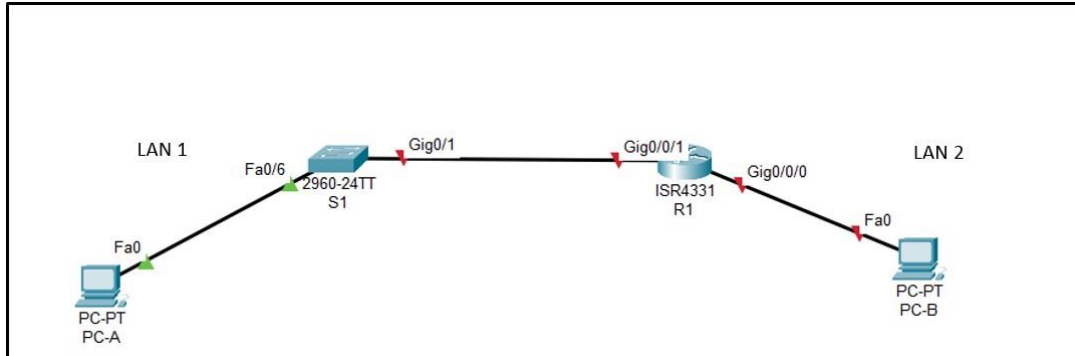
En el primer escenario se requiere realizar el subneteo VLSM (Variable Length Subnet Mask) para dos subredes LAN, con 60 host y 20 host para cada, y a partir de este proceso construir el esquema de direccionamiento IP para realizar la configuración básica y verificar la comunicación en cada subred.

En el segundo escenario se realizará la configuración de router y switch para lograr que cada dispositivo de la red coexistan con las configuración de las direcciones IP de los protocolos IPv4 al mismo tiempo con los protocolos de IPv6 (técnica dual-stack), así como la creación de VLANs, configuración de parámetros para servidor DHCP, entre otras configuraciones.

1. ESCENARIO No. 1

1.1 CONSTRUCCIÓN DE LA RED.

Figura 1. Topología escenario 1



Fuente: Propia

Se realiza la construcción de la topología en el simulador Packet Tracer, de acuerdo con los dispositivos y conexiones solicitadas para el escenario 1 en la guía.

1.2 DESARROLLO DEL ESQUEMA DE DIRECCIONAMIENTO IP.

Realizar el esquema de direccionamiento IP para la dirección IPv4 solicitada, creando las dos subredes con la cantidad requerida de hosts. Asignar las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1. Requerimientos direccionamiento

Ítem	Requerimiento
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host subred LAN1	60
Requerimiento de host subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1
R1 G0/0/0	Última dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1

Fuente: Guía Prueba de habilidades prácticas

Tabla 1. (Continuación)

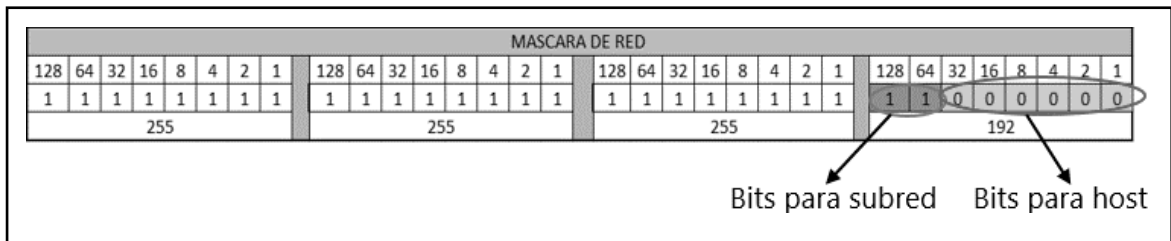
Item	Requerimiento
PC-A	Décima dirección de host de la subred LAN1
PC-B	Décima dirección de host de la subred LAN2

Fuente: Guía Prueba de habilidades prácticas

De acuerdo a los requerimientos de cantidad de host por subred se realiza el subneteo VLSM (Variable Length Subnet Mask) realizando el proceso para el cálculo de los host por red así:

Para la subred que solicita 60 host la máscara de subred queda de /26, porque se toman 2 bits del último octeto para un total de 26 bits, quedando la máscara de 255.255.255.192/26.

Figura 2. Cálculo máscara red LAN1



Fuente: Propia

Y se tienen 62 direcciones de host disponibles, porque se toma 2 bits del último octeto para red y los demás 6 bits quedan disponibles para direcciones de host, de acuerdo a la fórmula queda:

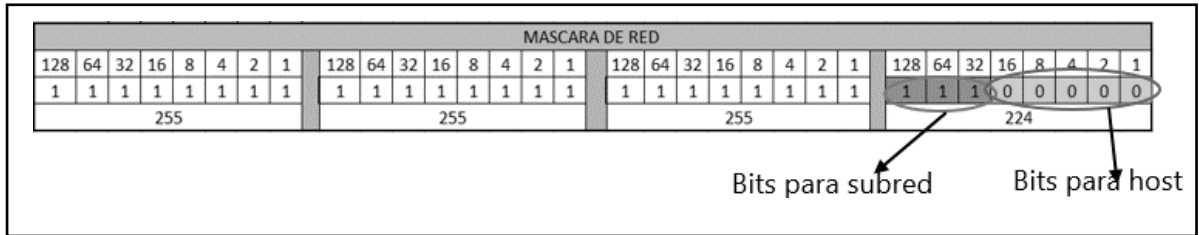
$2^n - 2 = \text{número de hosts}$, donde n es el número de host bits

$$2^6 = 64 - 2$$

$$= 62$$

Para la subred que solicita 20 host la máscara de subred queda de /27, porque se toman 3 bits del último octeto para subred, para un total de 27 bits, quedando la máscara de 255.255.255.224/27

Figura 3. Cálculo máscara red LAN2



Fuente: Propia

Y se tienen 30 direcciones de host disponibles, porque se toma 3 bits del último octeto para red y los demás 5 bits quedan disponibles para direcciones de host, de acuerdo a la fórmula queda:

$2^n - 2 = \text{número de hosts}$, donde n es el número de host bits

$2^5 = 32 - 2$

=30

De acuerdo al cálculo de subneteo VLSM se obteniendo los siguientes datos de la IPv4 172.84.3.0/24 para las dos subredes.

Tabla 2. Subneteo de redes

Host solicitados	Host obtenidos	Ip red	Primer host disponible	Ultimo host	Broadcast
60	62	172.84.3.0/26	172.84.3.1	172.84.3.62	172.84.3.63
20	30	172.84.3.64/27	172.84.3.65	172.84.3.94	172.84.3.95

Fuente: Propia

En la siguiente tabla se encuentra la información de las direcciones de IPv4 para cada uno de host de acuerdo con los requerimientos de la tabla No. 1.

Tabla 3. Direcciones IPv4 de los host

Item	Requerimiento
Dirección de Red	172.84.3.0
Requerimiento de host subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.84.3.62

Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas

Tabla 4. (Continuación)

Item	Requerimiento
R1 G0/0/0	172.84.3.94
S1 SVI	172.84.3.2
PC-A	172.84.3.10
PC-B	172.84.3.74

Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas

1.3 CONFIGURACIÓN DE ASPECTO BÁSICOS.

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

1.3.1 Router R1

Se configura el router de acuerdo a lo solicitado con:

1.3.2 Configuración desactivar la búsqueda DNS.

```
Router>enable
Router#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#
```

1.3.2.1 Nombre del router R1.

```
Router#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host
Router(config)#hostname R1
R1(config)#
R1#
```

1.3.2.2 Nombre del dominio: ccna-sa.com.

```
R1#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain name ccna-sa.com
R1(config)#
R1#
```

1.3.2.3 Contraseña cifrada para el modo EXEC privilegiado: ciscoenpass.

```
R1#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret ciscoenpass
R1(config)#
R1#
```

1.3.2.4 Contraseña de acceso a la consola: ciscoconpass.

```
R1#confi terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
```

1.3.2.5 Crear un usuario administrativo en la base de datos local: Nombre de usuario: admin Contraseña: admin1pass.

```
R1(config)#username admin secret admin1pass
R1(config)#
```

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

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#
```

1.3.2.7 Configurar las líneas VTY para que acepte únicamente las conexiones SSH.

```
R1(config-line)#transport input ssh
```

1.3.2.8 Cifrar las contraseñas de texto no cifrado.

```
R1(config)#service password-encryption
```

1.3.2.9 Configurar un banner MOTD: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

```
R1(config)#banner motd #Router 1 OLGA LUCIA CABALLERO MELGAREJO
PROGRAMA INGENIERIA DE SISTEMAS#
```

1.3.2.10 Configuración de interface G0/0/0: Establecer la descripción, establecer la dirección IPv4 y activar la interfaz.

```
R1(config)#interface gigabitEthernet 0/0/0
R1(config-if)#ip ad
R1(config-if)#ip address 172.84.3.94 255.255.255.224
R1(config-if)#no shutdown
```

1.3.2.11 Configuración de interface G0/0/1: Establecer la descripción, establecer la dirección IPv4 y activar la interfaz.

```
R1(config-if)#interface gigabitEthernet 0/0/1
R1(config-if)#ip address 172.84.3.62 255.255.255.192
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
```

1.3.2.12 Generar 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.ccsa-sa.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 1:45:41.271: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
```

1.3.3 Switch S1.

1.3.3.1 Desactivar la búsqueda DNS.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#
```

1.3.3.2 Nombre del router: S1.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#
```

1.3.3.3 Nombre del dominio: ccna-sa.com.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# ip domain name ccna-sa.com
S1(config)#
```

1.3.3.4 Contraseña cifrada para el modo EXEC privilegiado: ciscoenpass
Switch#configure terminal.

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

1.3.3.5 Contraseña de acceso a la consola: ciscoconpass.

```
S1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

1.3.3.6 Apagar todos los puertos sub usar: F0/1-4, F0/7-24, G0/1-2.

Los puertos requeridos ya se encuentran apagados, y no han sido activados mediante comandos ni les han sido conectados dispositivos.

1.3.3.7 Crear un usuario administrativo en la base de datos local: Nombre de usuario: admin Contraseña: admin1pass.

```
S1(config)#username admin secret admin1pass
S1(config)#
```

1.3.3.8 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
```

1.3.3.9 Configurar las líneas VTY para que acepte únicamente las conexiones SSH.

```
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

1.3.3.10 Cifrar las contraseñas de texto no cifrado.

```
S1(config)#service password-encryption
```

1.3.3.11 Configurar un banner MOTD: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

```
S1(config)#banner motd #Switch 1 Olga Lucia Caballero Melgarejo Ingeniería de
Sistemas#
```

1.3.3.12 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]
*Mar 1 2:30:49.864: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

1.3.3.13 Configure la interfaz de administración (SVI) en VALN1: Establecer la descripción y establecer la dirección IPv4.

```
Descripción
S1(config)# interface vlan 1
S1(config-if)#description CONEXIN RED LAN 1
```

Establecer la dirección IPv4

```
S1(config-if)#ip address 172.84.3.2 255.255.255.192
S1(config-if)#no shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

1.4 CONFIGURACIÓN DE LOS EQUIPOS.

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

1.4.1 Configuración de red de PC-A

De acuerdo a los requerimientos de cantidad de host por subred y la realización del subneteo VLSM (Variable Length Subnet Mask) se configura la PC-A y se registran los siguientes datos.

Tabla 5. Configuración PC-A

Ítem	Resultado
Descripción	PC-A
Dirección física	000C.853D.5A79
Dirección IPv4	172.84.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.84.3.62

Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas

1.4.2 Configuración de red de PC-B

De acuerdo a la configuración realizada para la PC-B se registran los siguientes datos.

Tabla 6. Configuración PC-B

Ítem	Resultado
Descripción	PC-B
Dirección física	0001.97E3.BD5D
Dirección IPv4	172.84.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.84.3.94

Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas

1.5 PRUEBA Y VERIFICACIÓN DE LA CONECTIVIDAD DE EXTREMO A EXTREMO

Se utiliza el comando ping para probar la conectividad entre todos los dispositivos de red, registrando los resultados en la tabla 6.

Tabla 7. Resultados pruebas ping

Ping desde	Ping A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.84.3.94	Exitoso
	R1 G0/0/1	172.84.3.62	Exitoso
	S1 VLAN1	172.84.3.2	Exitoso
	PC-B	172.84.3.74	Exitoso
PC-B	R1 G0/0/0	172.84.3.94	Exitoso
	R1 G0/0/1	172.84.3.62	Exitoso
	S1 VLAN1	172.84.3.2	Exitoso

Fuente: Propia, tomando como referencia Guía Prueba de habilidades prácticas

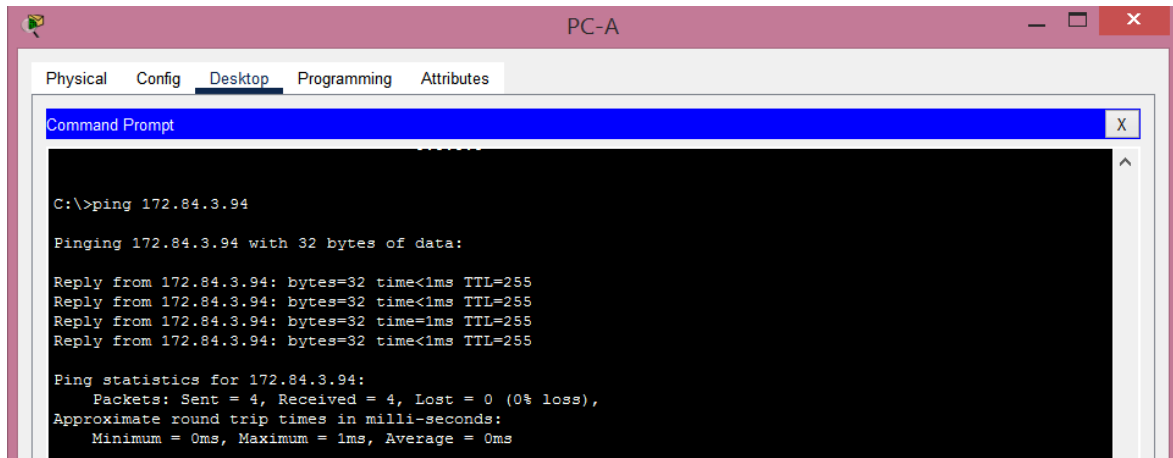
1.5.1 Ping desde PC-A a los hosts de la subred LAN1

Verificación de la comunicación entre los hosts de la subred LAN1, realizando pruebas mediante el comando ping a la cada una de las IP, obteniendo los siguientes resultados.

1.5.1.1 Desde PC-A(IP 172.84.3.10) a R1 G0/0/0 (IP 172.84.3.94): Exitoso.

Se verifica la existencia de comunicación entre la PC y las interfaces del router, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de la misma red.

Figura 4. Ping desde PC-A a R1 G0/0/0

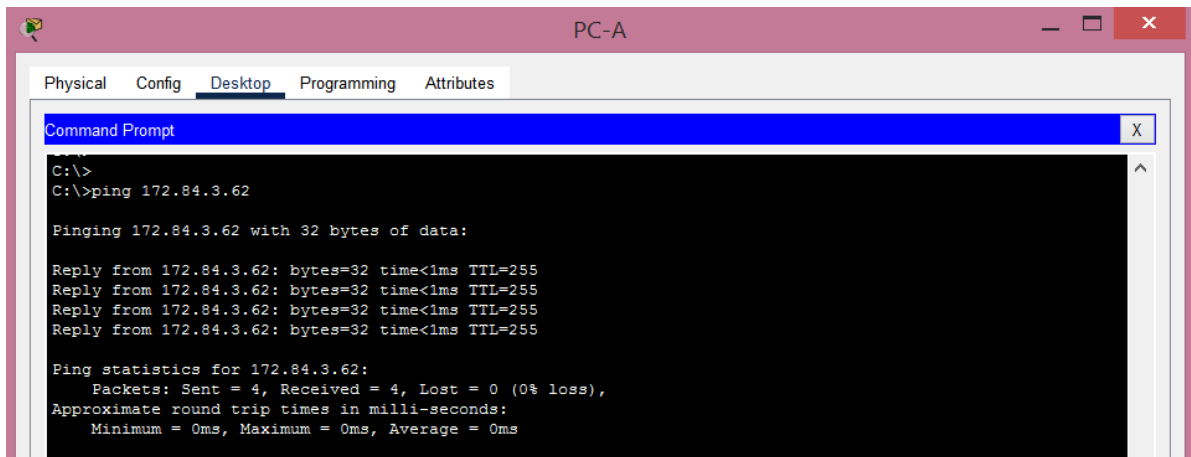


Fuente: Propia

1.5.1.2 Desde PC-A(IP 172.84.3.10) a R1 G0/0/1 (IP 172.84.3.62): Exitoso

Se verifica la existencia de comunicación entre la PC y las interfaces del router, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de la misma red.

Figura 5. Ping desde PC-A a R1 G0/0/1

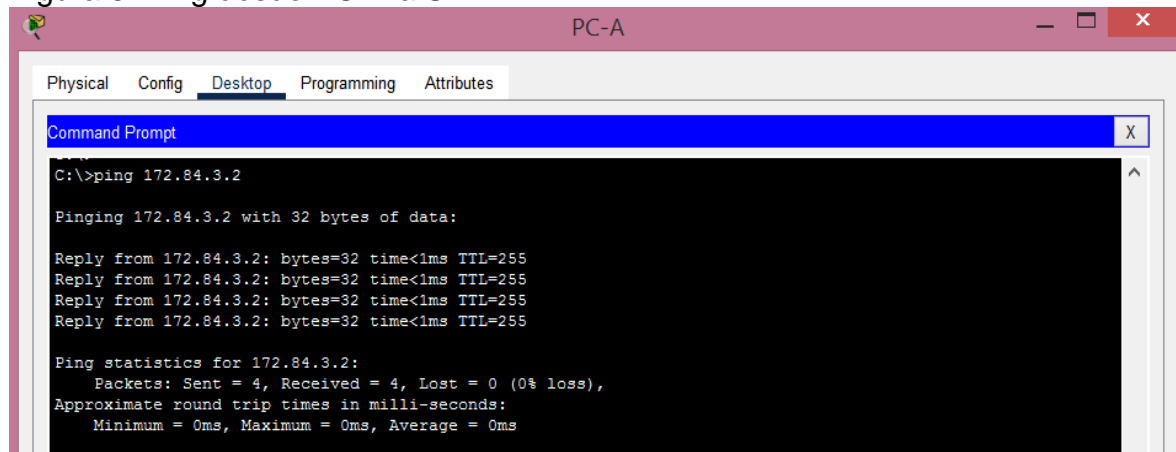


Fuente: Propia

1.5.1.3 Desde PC-A(IP 172.84.3.10) a S1 VLAN1 (172.84.3.2): Exitoso

Se verifica la existencia de comunicación entre la PC y las VLAN del switch, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de las dos subredes.

Figura 6. Ping desde PC-A a S1 VLAN1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.84.3.2

Pinging 172.84.3.2 with 32 bytes of data:

Reply from 172.84.3.2: bytes=32 time<1ms TTL=255
Reply from 172.84.3.2: bytes=32 time<1ms TTL=255
Reply from 172.84.3.2: bytes=32 time<1ms TTL=255
Reply from 172.84.3.2: bytes=32 time<1ms TTL=255

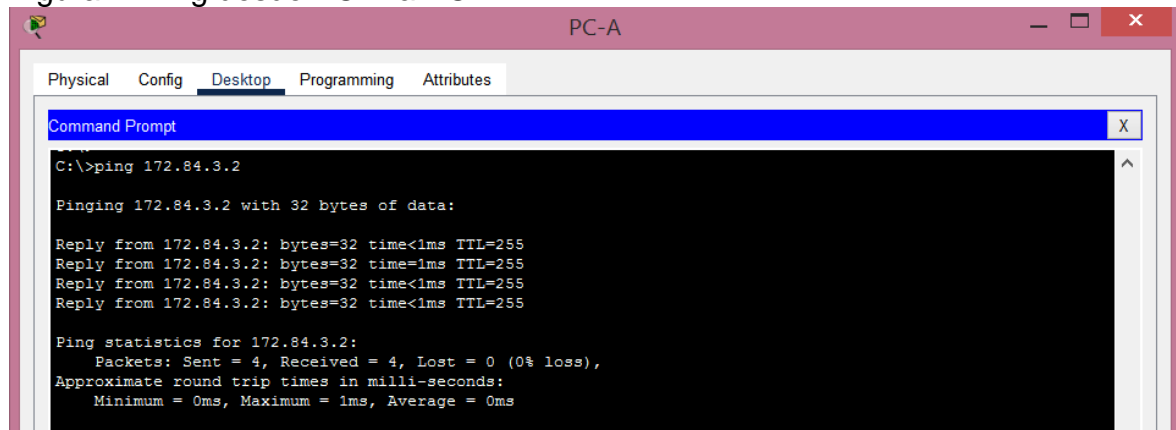
Ping statistics for 172.84.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Propia

1.5.1.4 Desde PC-A(IP 172.84.3.10) a PC-B (172.84.3.74): Exitoso

Se verifica la existencia de comunicación entre la PC y PC-B, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de las dos subredes.

Figura 7. Ping desde PC-A a PC-B



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.84.3.2

Pinging 172.84.3.2 with 32 bytes of data:

Reply from 172.84.3.2: bytes=32 time<1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time<1ms TTL=255
Reply from 172.84.3.2: bytes=32 time<1ms TTL=255

Ping statistics for 172.84.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Propia

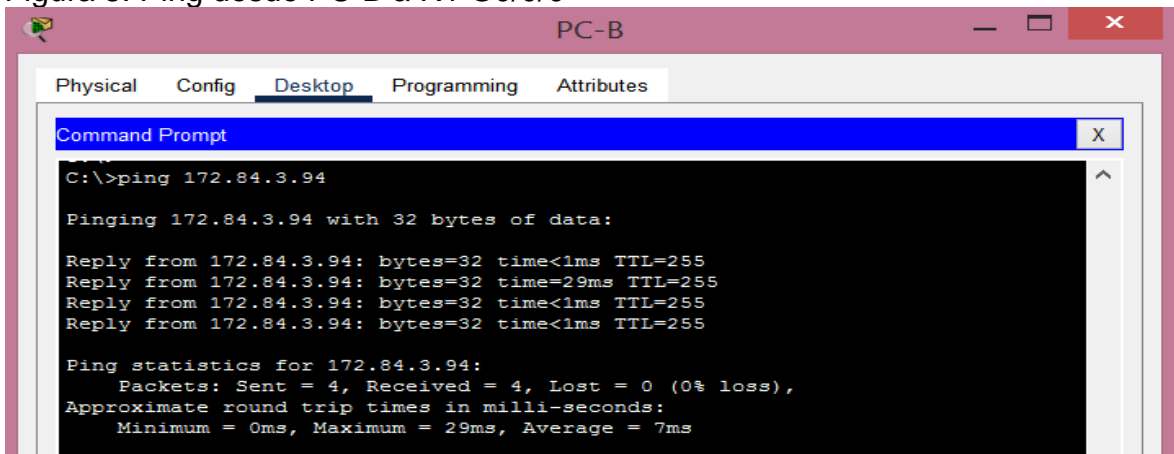
1.5.2 Ping desde PC-B a los host de la subred LAN2

Verificación de la comunicación entre los host de la subred LAN2, realizando pruebas mediante el comando ping a la cada una de las IP, obteniendo los siguientes resultados.

1.5.2.1 Desde PC-B(IP 172.84.3.74) a R1 G0/0/0 (IP 172.84.3.94): Exitoso

Se verifica la existencia de comunicación entre la PC y la interfaz del router, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de la red.

Figura 8. Ping desde PC-B a R1 G0/0/0



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.84.3.94

Pinging 172.84.3.94 with 32 bytes of data:

Reply from 172.84.3.94: bytes=32 time<1ms TTL=255
Reply from 172.84.3.94: bytes=32 time=29ms TTL=255
Reply from 172.84.3.94: bytes=32 time<1ms TTL=255
Reply from 172.84.3.94: bytes=32 time<1ms TTL=255

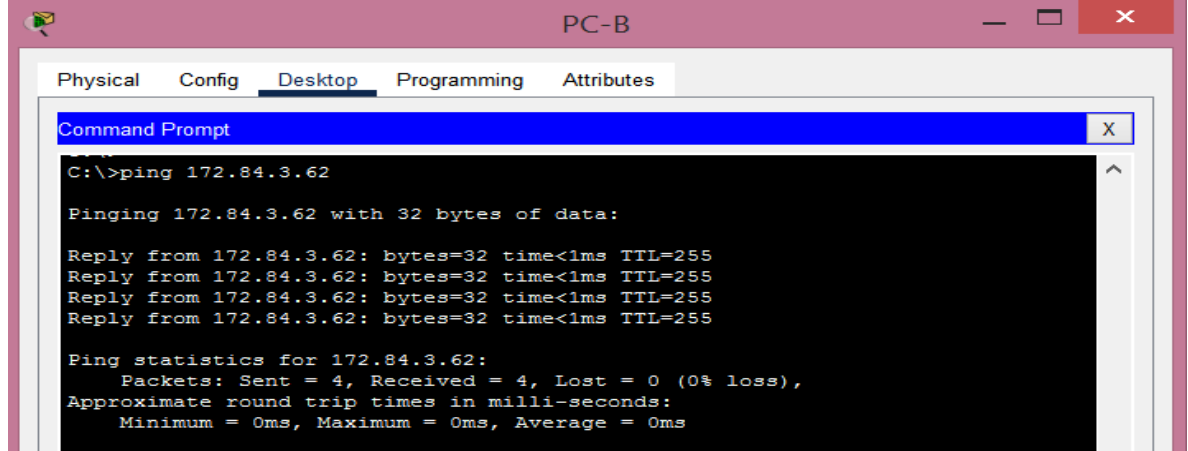
Ping statistics for 172.84.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 7ms
```

Fuente: Propia

1.5.2.2 Desde PC-B(IP 172.84.3.74) a R1 G0/0/1 172.84.3.62: Exitoso

Se verifica la existencia de comunicación entre la PC y la interfaz del router, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de la red.

Figura 9. Ping desde PC-B a R1 G0/0/1

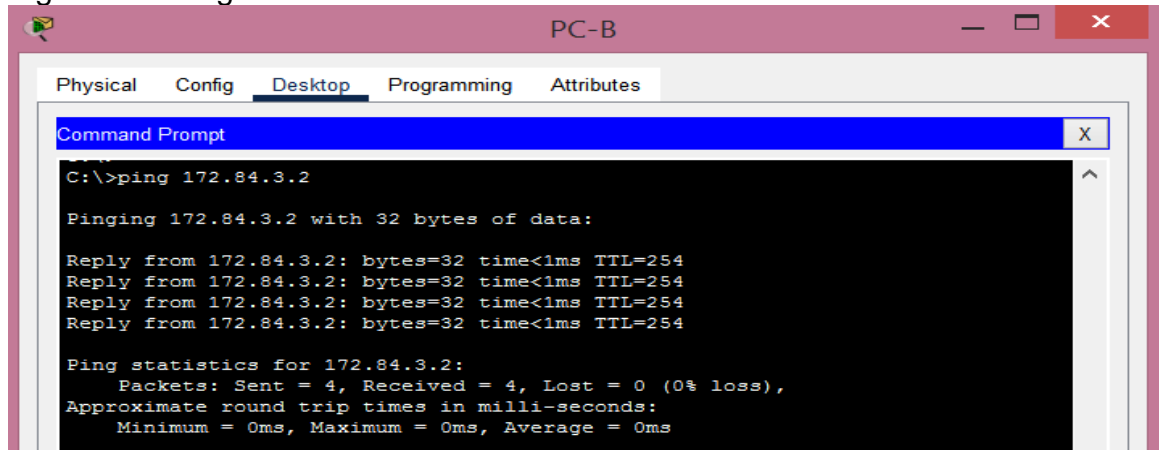


Fuente: Propia

1.5.2.3 Desde PC-B(IP 172.84.3.74) a S1 VLAN1 172.84.3.2: Exitoso

Se verifica la existencia de comunicación entre la PC y las VLAN del switch, lo cual obedece a la correcta configuración de las direcciones IP y la puerta de enlace, y se comprueba que los dos hosts se comunican dentro de las dos subredes.

Figura 10. Ping desde PC-B a S1 VLAN1

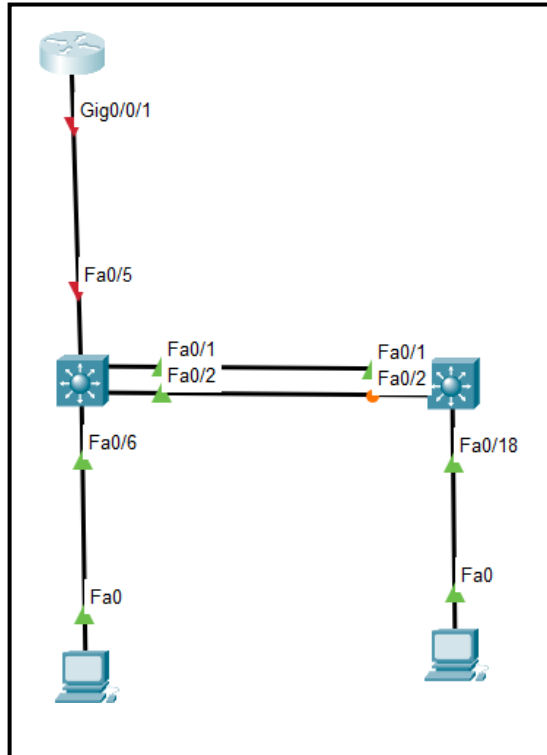


Fuente: Propia

2. ESCENARIO NO. 2

2.1 CONSTRUCCIÓN DE LA RED

Figura 11. Topología escenario 2



2.2 REQUERIMIENTOS

Tabla 8. VLAN

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

Fuente: Guía Prueba de habilidades prácticas

Tabla 9. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.84.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.84.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.84.8.97 /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	10.84.8.98 /29	10.84.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.84.8.99 /29	10.84.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Guía Prueba de habilidades prácticas

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

2.3 CONFIGURACIÓN ASPECTOS BASICOS

2.3.1 Realizar borrado de las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

2.3.1.1 Router

2.3.1.1.1 Borrado VLAN y configuraciones

```
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#
```

2.3.1.1.2 Inicialización

```
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...
Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly
System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
Current image running: Boot ROM0
```

2.3.1.2 Switch 1

2.3.1.2.1 Borrado VLAN y configuraciones

```
Switch>enable
Switch#delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (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#
```

2.3.1.2.2 Inicialización

```
Switch#reload
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 0001.4346.64A1
Xmodem file system is available.
Initializing Flash...
```

2.3.1.3 Switch 2

2.3.1.3.1 Borrado VLAN y configuraciones

```
Switch>enable
Switch#delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (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#
```

2.3.1.3.2 Inicialización

```
Switch#reload
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 0001.4346.64A1
Xmodem file system is available.
```

Initializing Flash...

2.3.2 Configuración la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

2.3.2.1 Switch 1.

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
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)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
```

2.3.2.2 Switch 2.

```
Switch>enable
Switch#configure terminal
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
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)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 00E0.F914.AEEC
Xmodem file system is available.
```

Initializing Flash...

2.4 CONFIGURACIÓN DEL R1.

2.4.1 Desactivar la búsqueda DNS.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
```

2.4.2 Nombre del router.

```
Router(config)#hostname R1
R1(config)#
```

2.4.3 Nombre de dominio: ccna-sa.com.

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

2.4.4 Contraseña cifrada para el modo EXEC privilegiado: class.

```
R1(config)#enable secret class
```

2.4.5 Contraseña de acceso a la consola: cisco.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

2.4.6 Establecer la longitud mínima para las contraseñas: 5 caracteres

```
R1(config)#security passwords min-length 5.
```

2.4.7 Crear un usuario administrativo en la base de datos local. Nombre de usuario: admin Password: admin1pass.

```
R1(config)#username admin secret admin1pass
```

2.4.8 Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.

```
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#exit
```

2.4.9 Configurar VTY solo aceptando SSH.

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
```

2.4.10 Cifrar las contraseñas de texto no cifrado

```
R1(config)#service password-encryption
R1(config)#
```

2.4.11 Configure un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

```
R1(config)#banner motd #R1-OLGA LUCIA CABALLERO MELGAREJO-
INGENIERIA DE SISTEMAS#
R1(config)#
```

2.4.12 Habilitar el routing IPv6

```
R1(config)#ipv6 unicast-routing
```

2.4.13 Configurar interfaz G0/0/1 y subinterfaces:

Se realiza la configuración de acuerdo a las siguientes especificaciones: establecer la descripción, establecer la dirección IPv4, establecer la dirección local de enlace IPv6 como fe80::1, establecer la dirección IPv6 y activar la interfaz.

2.4.13.1 Interface Docentes:

```
R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 uni
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#description Docentes
R1(config-subif)#ip address 10.84.8.1 255.255.255.192
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)#
```

2.4.13.2 Interface Estudiantes.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#description Estudiantes
R1(config-subif)#ip address 10.84.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
```

2.4.13.3 Interface Invitados

```
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.40
```

```
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#description Invitados
R1(config-subif)#ip address 10.84.8.97 255.255.255.248
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)#
```

2.4.13.4 Interface Native

```
R1(config)#interface g0/0/1
R1(config-if)#int g0/0/1.56
R1(config-subif)#encapsulation dot1Q 56
R1(config-subif)#description Native
R1(config-subif)#exit
R1(config)#interface g0/0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface g0/0/1
R1(config-if)#no shutdown
R1(config-if)#
```

2.4.14 Configure el Loopback0 interface.

Se realiza la configuración de acuerdo a las siguientes especificaciones: establecer la dirección IPv4, establecer la dirección IPv6 y establecer la dirección local de enlace IPv6 como fe80::1.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#description 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)#
```

2.4.15 Generar una clave de cifrado RSA-Módulo de 1024 bits.

```
R1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R1.ccna-lab.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 1:31:4.501: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
```

2.5 CONFIGURACIÓN DEL S1.

2.5.1 Desactivar la búsqueda DNS.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
```

2.5.2 Nombre del switch:S1.

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

2.5.3 Nombre de dominio: ccna-sa.com.

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

2.5.4 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
S1(config-line)#exit
S1(config)#
```

2.5.5 Crear un usuario administrativo en la base de datos local. Nombre de usuario: admin Password: admin1pass.

```
S1(config)#username admin secret admin1pass
```

2.5.6 Configurar 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
```

2.5.6.1 Configurar las líneas VTY para que acepten únicamente las conexiones SSH.

```
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

2.5.7 Cifrar las contraseñas de texto no cifrado.

```
S1(config)#service password-encryption
```

2.5.8 Configurar un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

```
S1(config)#banner motd "SWITCH 1-OLGA LUCIA CABALLERO MELGAREJO-
ING SISTEMAS"
```

2.5.9 Generar una clave de cifrado RSA: Módulo de 1024 bits.

```
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 0:28:1.165: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

2.5.10 Configurar la interfaz de administración (SVI) con las siguientes especificaciones: establecer la dirección IPv4 de capa 3, establecer la dirección local de enlace IPv6 como FE80::98 para S1, establecer la dirección IPv6 de capa 3.

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ipv6 unicast-routing
S1(config)#interface vlan 40
S1(config-if)#ip address 10.84.8.98 255.255.255.248
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)#
```

2.5.11 Configuración del gateway predeterminado, configurando la puerta de enlace predeterminada como 10.84.8.97 para IPv4

```
S1(config)#ip default-gateway 10.84.8.97
```

2.6 CONFIGURACIÓN DEL S2

2.6.1 Desactivar la búsqueda DNS.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
```

2.6.2 Nombre del switch S2.

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

2.6.3 Nombre de dominio: ccna-sa.com.

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

2.6.4 Contraseña cifrada para el modo EXEC privilegiado: class

```
S2(config)#enable secret class
```

2.6.5 Contraseña de acceso a la consola: cisco.

```
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#
```

2.6.6 Crear un usuario administrativo en la base de datos local. Nombre de usuario: admin Password: admin1pass

```
S2(config)#user admin secret admin1pass
```

2.6.7 Configurar 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
```

2.6.8 Configurar las líneas VTY para que acepten únicamente las conexiones SSH.

```
S2(config-line)#transport input ssh
S2(config-line)#exit
```

2.6.9 Cifrar las contraseñas de texto no cifrado.

```
S2(config)#service password-encryption
```

2.6.10 Configurar un MOTD Banner: Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

```
S2(config)#banner motd "SWITCH 2-OLGA LUCIA CABALLERO MELGARJE-
ING SISTEMAS"
```

2.6.11 Generar 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 1:20:25.526: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#
```

2.6.12 Configurar la interfaz de administración (SVI) con las siguientes especificaciones: establecer la dirección IPv4 de capa 3, establecer la dirección local de enlace IPv6 como FE80::99 para S2 y establecer la dirección IPv6 de capa 3.

```
S2(config)#ipv6 unicast-routing
S2(config)#interface vlan 40
S2(config-if)#ip address 10.84.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#exit
```

2.6.13 Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.84.8.97 para IPv4.

```
S2(config)#ip default-gateway 10.84.8.97
S2(config)#
```

2.7 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

2.7.1 Configuración del S1.

La configuración del S1 incluye las siguientes tareas y códigos.

2.7.1.1 Crear VLANs.

VLAN 20, nombre Docentes

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

VLAN 30, nombre Estudiantes

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

VLAN 40, nombre Invitados

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

```
S1(config-vlan)#name Invitados
S1(config-vlan)#exit
S1(config)#
```

VLAN 50, nombre Usuarios

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

VLAN 56, nombre Native

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

Verificación de creación de las VLANs.

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  
S1#
```

2.7.1.2 Crear troncos 802.1Q que utilicen la VLAN 56 nativa: Interfaces F0/1, F0/2 y F0/5

Interface F0/1

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface f0/1

S1(config-if)#switchport trunk encapsulation dot1Q

S1(config-if)#switchport mode trunk

S1(config-if)#

%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 Vlan40, changed state to up

S1(config-if)#switchport trunk Native vlan 56

S1(config-if)#exit

S1(config)#

Interfaces F0/2

S1(config)#interface f0/2

S1(config-if)#switchport trunk encapsulation dot1Q

```
S1(config-if)#switchport mode trunk
S1(config-if)#
%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)#switchport trunk Native vlan 56
S1(config-if)#exit
S1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/2 (56), with S2 FastEthernet0/2 (1)
```

Interfaces F0/5

```
S1(config)#interface f0/5
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to up
S1(config-if)#switchport trunk Native vlan 56
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/2 (56)switchport trunk encapsulation dot1Q
S1(config-if)#exit
S1(config)#
```

La siguiente corresponde a la comprobación de configuración y uso de la VLAN 56 Nativa para cada una de las interfaces solicitadas.

```
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
```

2.7.1.3 Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, usar el protocolo LACP para la negociación

```
S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1
S1(config-if-range)#exit
S1(config)#interface port-channel 1
S1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 20,30,40,50,56
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

2.7.1.4 Configurar el puerto de acceso de host para VLAN 20 para la Interface F0/6.

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show vlan brief
```

VLAN Name Status Ports

```
-----
1 default active Po1, Fa0/1, Fa0/2, 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
```

2.7.1.5 Configurar la seguridad del puerto en los puertos de acceso: Permitir 4 direcciones MAC.

```
S1(config)#interface 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
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

2.7.1.6 Proteja todas las interfaces no utilizadas. Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#description interfaces no utilizadas
S1(config-if-range)#shutdown
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#
```

2.7.2 Configuración de S2.

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

2.7.2.1 Crear VLAN

```
VLAN 20, nombre Docentes
S2(config)#vlan 20
S2(config-vlan)#name Docentes
S2(config-vlan)#exit
S2(config)#
```

```
VLAN 30, nombre Estudiantes
S2(config)#vlan 30
S2(config-vlan)#name Estudiantes
S2(config-vlan)#exit
S2(config)#
```

```
VLAN 40, nombre Invitados
S2(config)#vlan 40
S2(config-vlan)#name Invitados
S2(config-vlan)#exit
S2(config)#
```

```
VLAN 50, nombre Usuarios
S2(config)#vlan 50
S2(config-vlan)#name Usuarios
S2(config-vlan)#exit
```

```

S2(config)#
VLAN 56, nombre Native
S2(config)#vlan 56
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#

```

Mediante el siguiente código se verifica la Configuración realizada de las VLANs.

```
S2#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

```

2.7.2.2 Crear troncos 802.1Q que utilicen la VLAN 56 nativa Interfaces F0/1 y F0/2.

```
Interface F0/1
```

```
S2#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
S2(config)#interface f0/1
```

```
S2(config-if)#switchport trunk encapsulation dot1Q
```

```
S2(config-if)#switchport mode trunk
```

```
S2(config-if)#
```

```
%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 Vlan40, changed state to up
```

```
S2(config-if)#switchport trunk Native vlan 56
S2(config-if)#exit
S2(config)#
```

Interface F0/2

```
S2(config)#interface f0/2
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#
%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
S2(config-if)#switchport trunk Native vlan 56
S2(config-if)#exit
S2(config)#
```

La siguiente corresponde a la comprobación de configuración y uso de la VLAN 56 Nativa.

```
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

2.7.2.3 Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, usando el protocolo LACP para la negociación

```
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
%EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be
suspended (native vlan of Fa0/1 is 56, Po1 id 1)
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to
down
%EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be
suspended (native vlan of Fa0/2 is 56, Po1 id 1)
S2(config-if-range)#exit
S2(config)#interface port-channel 1
S2(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
S2(config-if)#switchport trunk encapsulation dot1Q
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
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

2.7.2.4 Configurar el puerto de acceso del host para la VLAN 30-Interfaz F0/18.

```
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
S2#
%SYS-5-CONFIG_I: Configured from console by console

```

Mediante el siguiente código se realiza la verificación de la Configuración de las interfaces:

```
S2#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Po1, 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	

2.7.2.5 Configure port-security en los access ports, permite 4 MAC addresses.

```

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 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)#exit
S2

```

2.7.2.6 Asegure todas las interfaces no utilizadas. Asignar a VLAN 50, establecer en modo de acceso, agregar una descripción y apagar.

```

S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range g0/1-2, f0/3-4, f0/7-24

```

```
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 50
S2(config-if-range)#description interfaces no utilizadas
S2(config-if-range)#shutdown
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
```

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S2(config-if-range)#

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to down

S2(config-if-range)#switchport port-security

S2(config-if-range)#switchport port-security violation shutdown

S2(config-if-range)#exit

S2(config)#exit

S2#

%SYS-5-CONFIG_I: Configured from console by console

2.8 CONFIGURAR SOPORTE DE HOST

Las siguientes tareas y códigos de configuración para R1:

2.8.1 Configurar Default Routing creando rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, los cuales fueron realizados en pasos anteriores.

2.8.2 Configurar IPv4 DHCP para VLAN 20: Creando 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 especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#ip dhcp pool vlan20
```

```
R1(dhcp-config)#network 10.84.8.0 255.255.255.192
```

```
R1(dhcp-config)#default-router 10.84.8.1
```

```
R1(dhcp-config)#domain-name unad-ccna-sa.net
```

```
R1(dhcp-config)#ip dhcp excluded-address 10.84.8.2 10.84.8.51
```

R1(config)#

2.8.3 Configurar DHCP IPv4 para VLAN 30. Creando un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asignar el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan30
R1(dhcp-config)#network 10.84.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.84.8.65
R1(dhcp-config)#domain-name unad-ccna-sa.net
R1(dhcp-config)#ip dhcp excluded-address 10.84.8.66 10.84.8.83
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

2.9 CONFIGURAR LOS SERVIDORES

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

Tabla 10. Configuración de red de PC-A

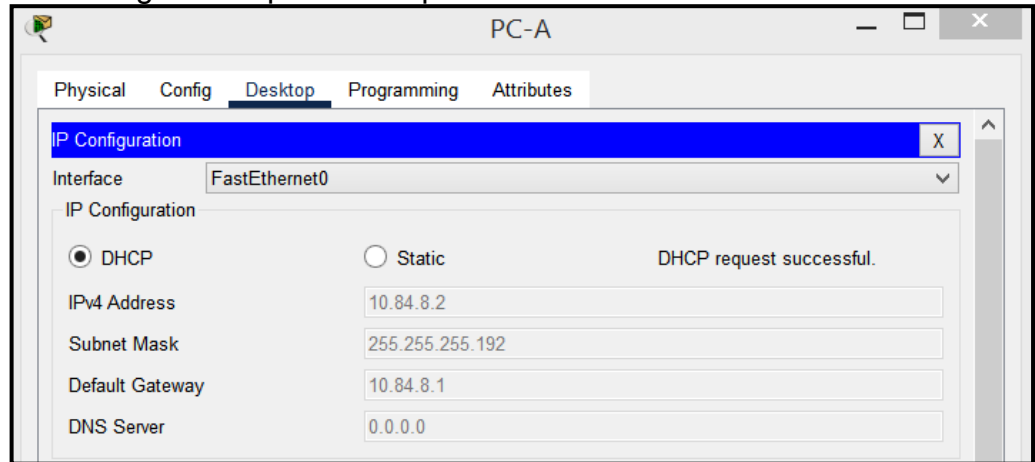
Descripción	Dirección IP
Dirección física	00D0.975C.89DB
Dirección IP	10.84.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.84.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Propia

2.9.1 IPv4 configuración por DHCP para la PC-A.

De acuerdo a la configuración realizada para el router la siguiente corresponde a la configuración de las direcciones IPv4 para la PC-A.

Figura 12. Configuración por DHCP para PC-A

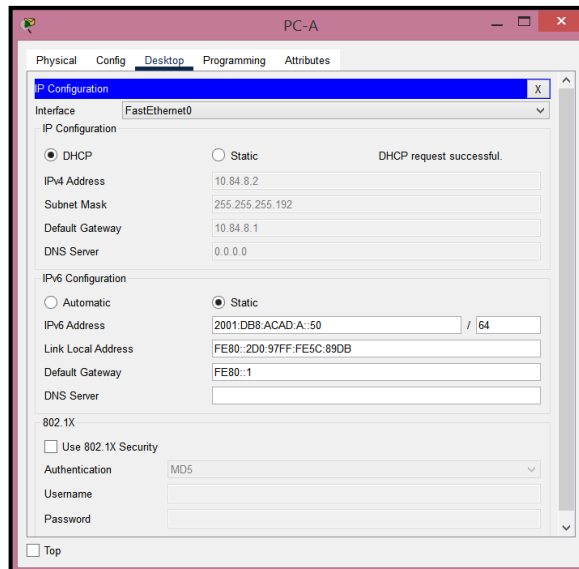


Fuente: Propia

2.9.2 IPv6 configuración estática para la PC-A.

Para las direcciones IPv6 se configuran de acuerdo a las especificaciones suministradas.

Figura 13. Configuración IPv6 de PC-A



Fuente: Propia

Tabla 11. Configuración de red de PC-B

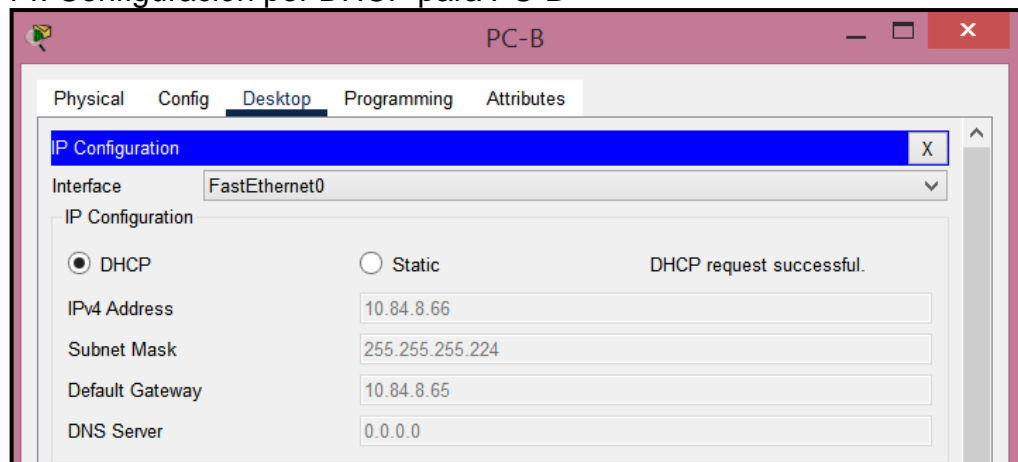
Descripción	Dirección IP
Dirección física	0001.4353.D2E5
Dirección IP	10.84.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Propia

2.9.3 IPv4 configuración por DHCP para la PC-B.

De acuerdo a la configuración realizada para el router la siguiente corresponde a la configuración de las direcciones IPv4 para la PC-B.

Figura 14. Configuración por DHCP para PC-B

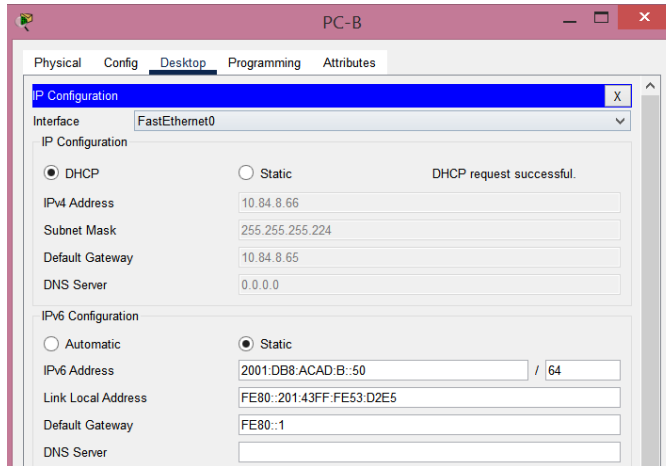


Fuente: Propia

2.9.4 IPv6 configuración estática para la PC-B.

Para las direcciones IPv6 se configuran de acuerdo a las especificaciones suministradas.

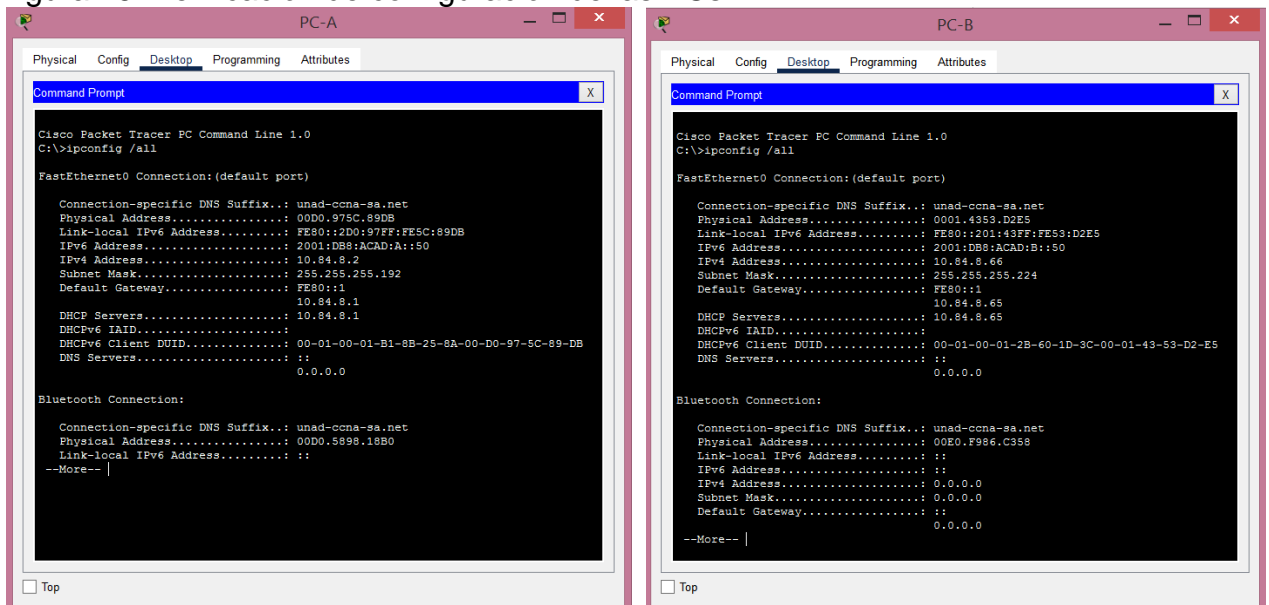
Figura 15. Configuración IPv6 de PC-B



Fuente: Propia

Con el comando ipconfig /all se verifica la configuración de las PC-A y PC-B.

Figura 16. Verificación de configuración de las PCs



Fuente: Propia

2.10 PRUEBAS DE CONECTIVIDAD DE EXTREMO A EXTREMO

Usando el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. Utilizando la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 12. Resultados de verificación de conexión

Desde	A		Dirección IP	Resultados
PC-A	R1, G0/0/1.20	IPv4	10.84.8.1	Exitoso
		IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.30	IPv4	10.84.8.65	Exitoso
		IPv6	2001:db8:acad:b::1	Exitoso
	R1, G0/0/1.40	IPv4	10.84.8.97	Exitoso
		IPv6	2001:db8:acad:c::1	Exitoso
	S1, VLAN 40	IPv4	10.84.8.98	Exitoso
		IPv6	2001:db8:acad:c::98	Fallido
	S2, VLAN 40	IPv4	10.84.8.99	Exitoso
		IPv6	2001:db8:acad:c::99	Fallido
	PC-B	IPv4	10.84.8.66	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	10.84.8.1	Exitoso
		IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.30	IPv4	10.84.8.65	Exitoso
		IPv6	2001:db8:acad:b::1	Exitoso
	R1, G0/0/1.40	IPv4	10.84.8.97	Exitoso
		IPv6	2001:db8:acad:c::1	Exitoso
	S1, VLAN 40	IPv4	10.84.8.98	Exitoso
		IPv6	2001:db8:acad:c::98	Fallido
	S2, VLAN 40	IPv4	10.84.8.99	Exitoso
		IPv6	2001:db8:acad:c::99	Fallido

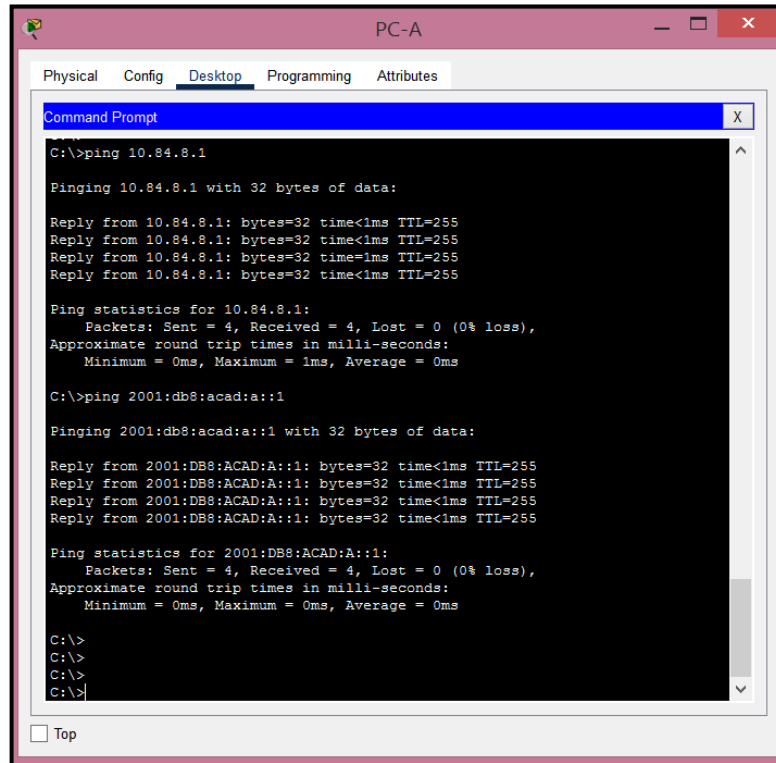
Fuente: Propia

2.10.1 Ping desde PC-A a R1 a la Interface G0/0/1.20 IPv4 (10.84.8.1) e IPv6 (2001:db8:acad:a::1).

Se verifica la existencia de comunicación entre la PC-A y el router R1 en la interface G0/0/1.20, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 20 (Docentes), así mismo se comprueba que los dos

hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 17. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.20



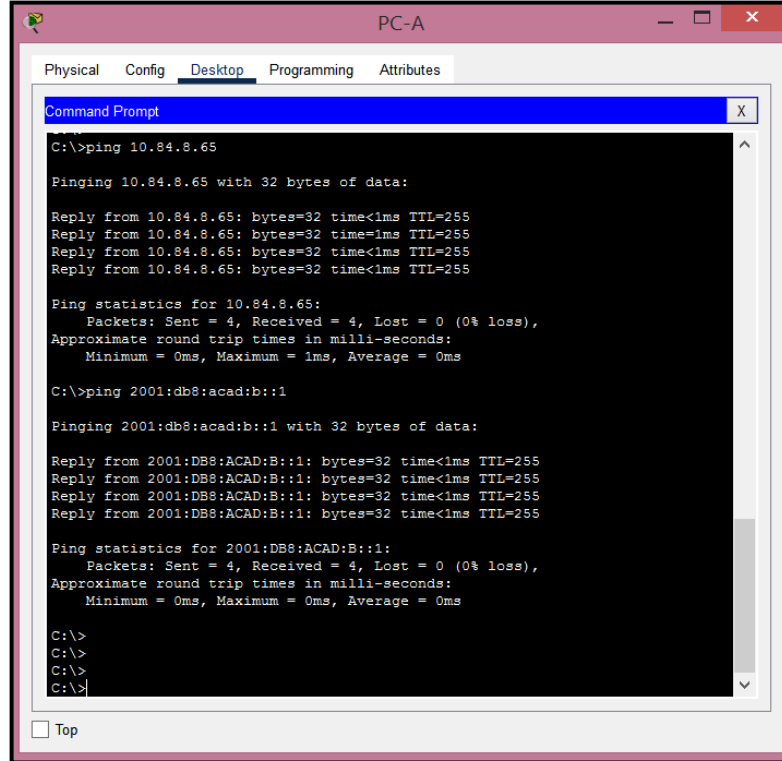
```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.84.8.1
Pinging 10.84.8.1 with 32 bytes of data:
Reply from 10.84.8.1: bytes=32 time<1ms TTL=255
Reply from 10.84.8.1: bytes=32 time<1ms TTL=255
Reply from 10.84.8.1: bytes=32 time<1ms TTL=255
Reply from 10.84.8.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.84.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:a::1
Pinging 2001:db8:acad:a::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

2.10.2 Ping desde PC-A a R1 interface G0/0/1.30 IPv4 (10.84.8.65) e IPv6 (2001:db8:acad:b::1)

Se verifica la existencia de comunicación entre la PC-A y el router R1 en la interface G0/0/1.30, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 30 (Estudiantes), así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 18. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.30



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.84.8.65

Pinging 10.84.8.65 with 32 bytes of data:

Reply from 10.84.8.65: bytes=32 time<1ms TTL=255
Reply from 10.84.8.65: bytes=32 time<1ms TTL=255
Reply from 10.84.8.65: bytes=32 time<1ms TTL=255
Reply from 10.84.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.84.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

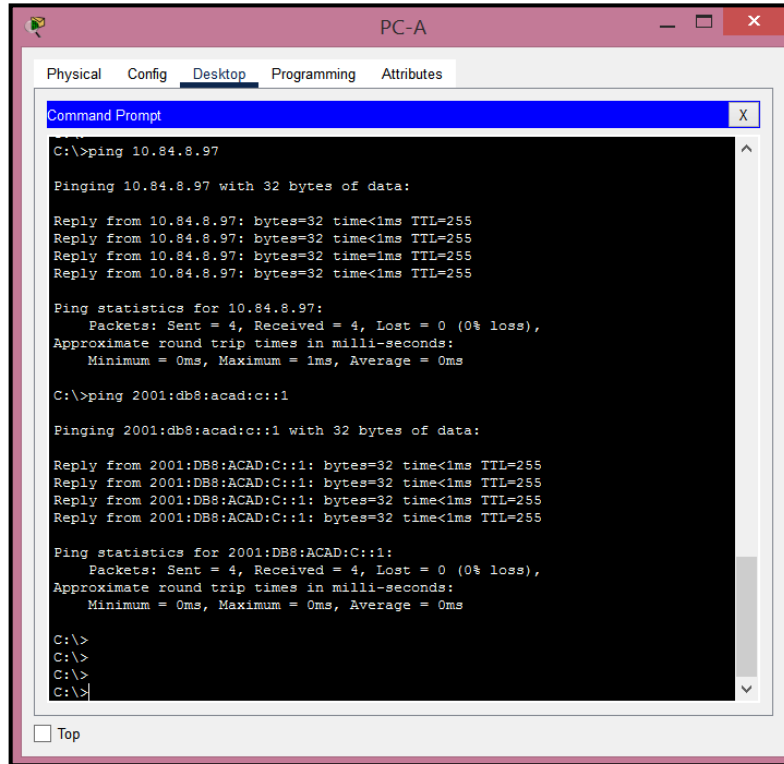
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

2.10.3 Ping desde PC-A a R1 interface G0/0/1.40 IPv4 (10.84.8.97) e IPv6 (2001:db8:acad:c::1)

Se verifica la existencia de comunicación entre la PC-A y el router R1 en la interface G0/0/1.40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados), así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 19. Verificación comunicación IPv4 e IPv6 desde PC-A a G0/0/1.40



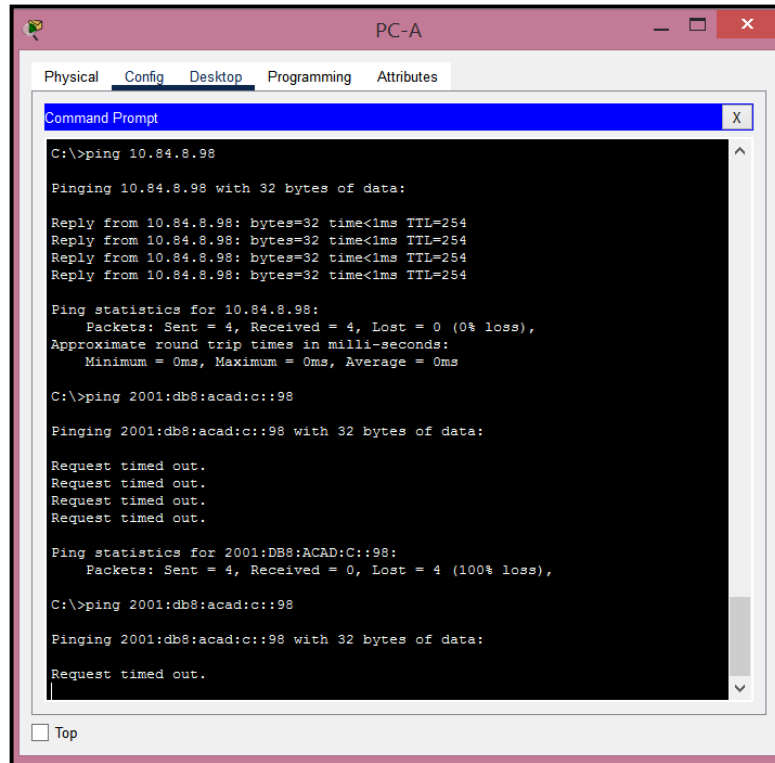
```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.84.8.97
Pinging 10.84.8.97 with 32 bytes of data:
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Ping statistics for 10.84.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:c::1
Pinging 2001:db8:acad:c::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

2.10.4 Ping desde PC-A al S1 VLAN 40 IPv4 (10.84.8.98) e IPv6 (2001:db8:acad:c::98).

Se verifica la existencia de comunicación entre la PC-A y el switch S1 en la interface VLAN40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados) para IPv4. Para IPv6 no hay conexión debido a una limitación del IOS del simulador.

Figura 20. Verificación comunicación IPv4 e IPv6 desde PC-A a S1 VLAN-40

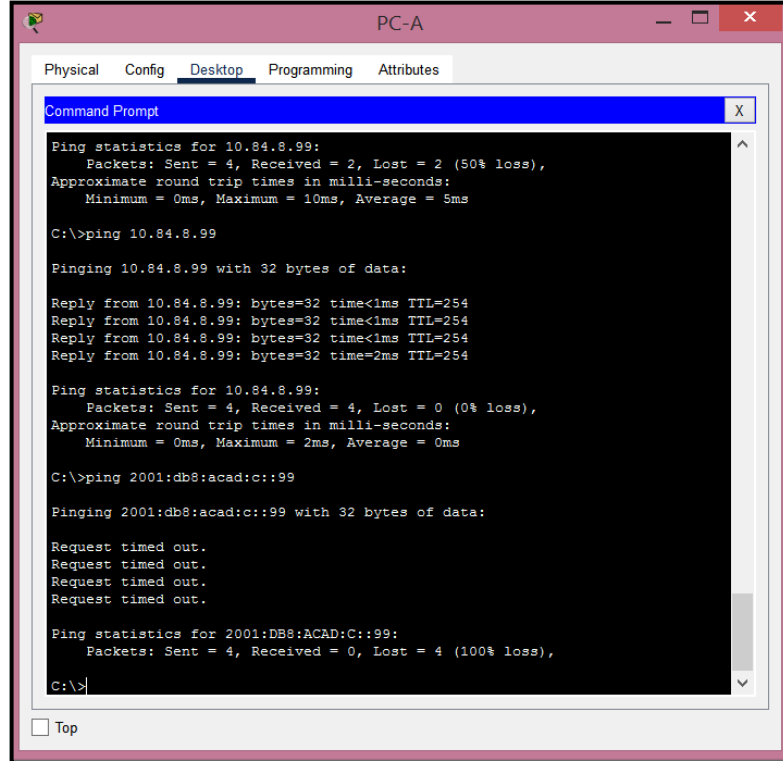


Fuente: Propia

2.10.5 Ping desde PC-A a S2 VLAN 40 IPv4 (10.84.8.99) e IPv6 (2001:db8:acad:c::99)

Se verifica la existencia de comunicación entre la PC-A y el switch S2 en la interface VLAN40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados) para IPv4. Para IPv6 no hay conexión debido a una limitación del IOS del simulador.

Figura 21. Verificación comunicación IPv4 e IPv6 desde PC-A a S2 VLAN-40

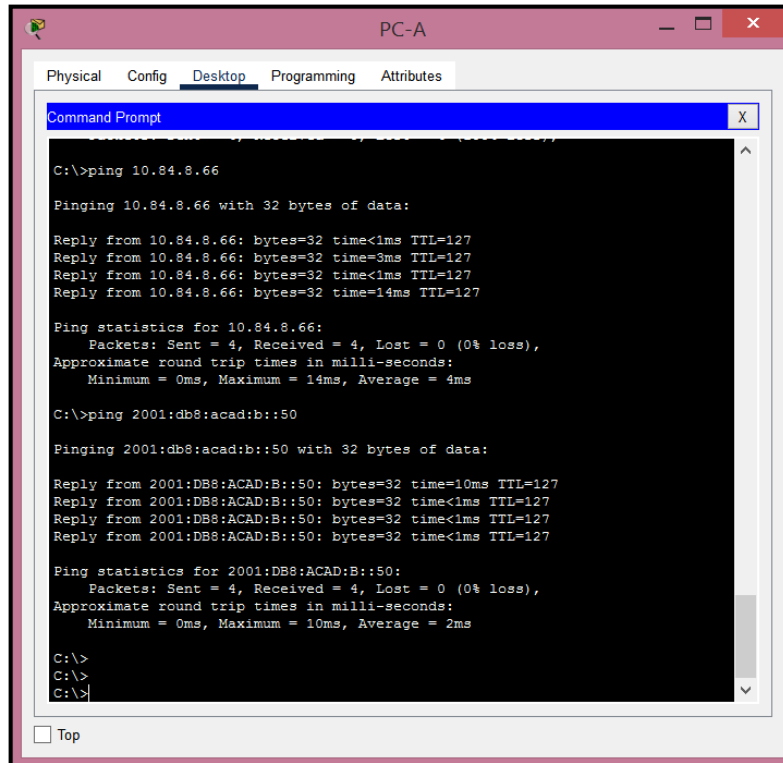


Fuente: Propia

2.10.6 Ping desde PC-A a PC-B IPv4 (10.84.8.66) e IPv6 (2001:db8:acad:b::50)

Se verifica la existencia de comunicación entre la PC-A y la PC-B, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, las VLANs, así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el Ipv6, como consecuencia de la configuración de SDM en el switch para que admita Ipv6, entre otras configuraciones dentro del router como habilitar el routing Ipv6.

Figura 22. Verificación de comunicación PC-A a PC-B

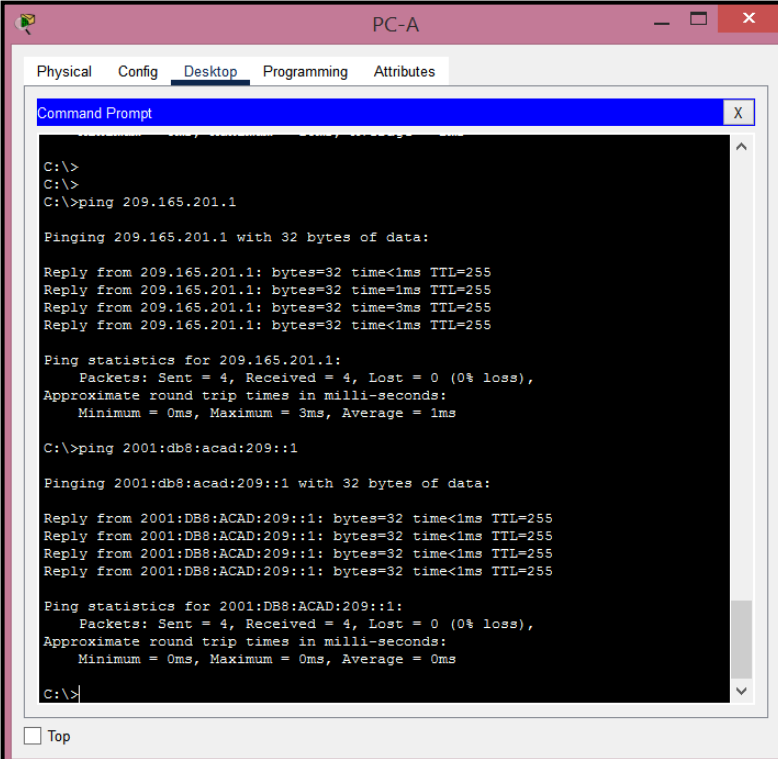


Fuente: propia

2.10.7 Ping desde PC-A a R1 Bucle 0 (209.165.201.1) e IPv6 (2001:db8:acad:209::1).

Se verifica la existencia de comunicación entre la PC-A y el R1 Bucle 0, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, las VLANs, así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el Ipv6, como consecuencia de la configuración de SDM en el switch para que admita Ipv6, entre otras configuraciones dentro del router como habilitar el routing Ipv6 y la configuración de la IP de loopback.

Figura 23. Verificación de comunicación de PC-A a R1 Bucle 0



```
C:\>
C:\>
C:\>ping 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=3ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Propia

2.10.8 Ping desde PC-B a R1 Bucle 0 (209.165.201.1) e IPv6 (2001:db8:acad:209::1)

Se verifica la existencia de comunicación entre la PC-B y el R1 Bucle 0, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, las VLANs, así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el Ipv6, como consecuencia de la configuración de SDM en el switch para que admita Ipv6, entre otras configuraciones dentro del router como habilitar el routing Ipv6 y la configuración de la IP de loopback.

Figura 24. Verificación de comunicación de PC-B a R1 Bucle 0

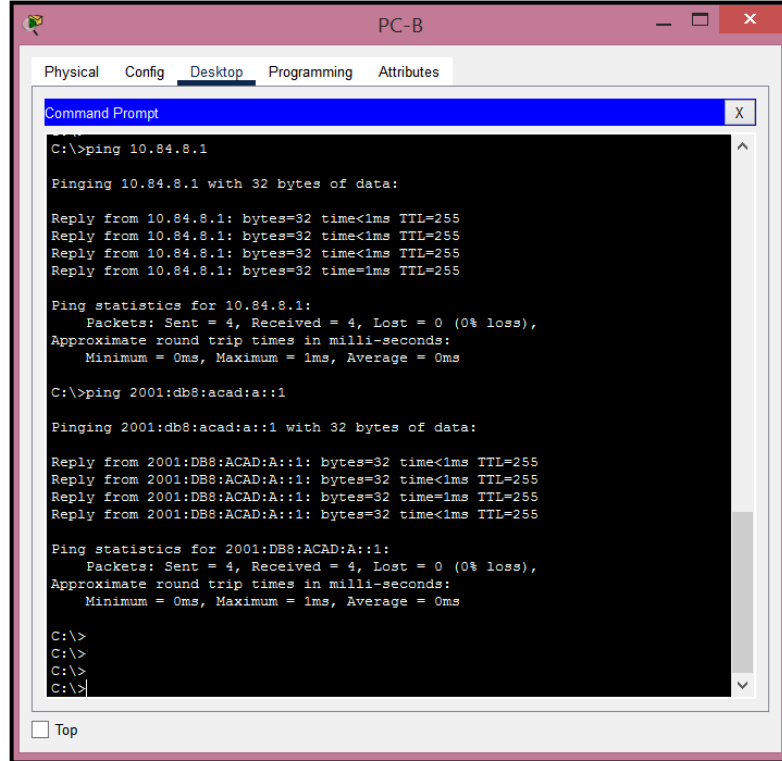
```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:db8:acad:209::1
Pinging 2001:db8:acad:209::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

2.10.9 Ping desde PC-B a R1 G0/0/1.20 IPv4 (10.84.8.1) e IPv6 (2001:db8:acad:a::1)

Se verifica la existencia de comunicación entre la PC-B y el router R1 en la interface G0/0/1.20, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 20 (Docentes), así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 25. Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.20

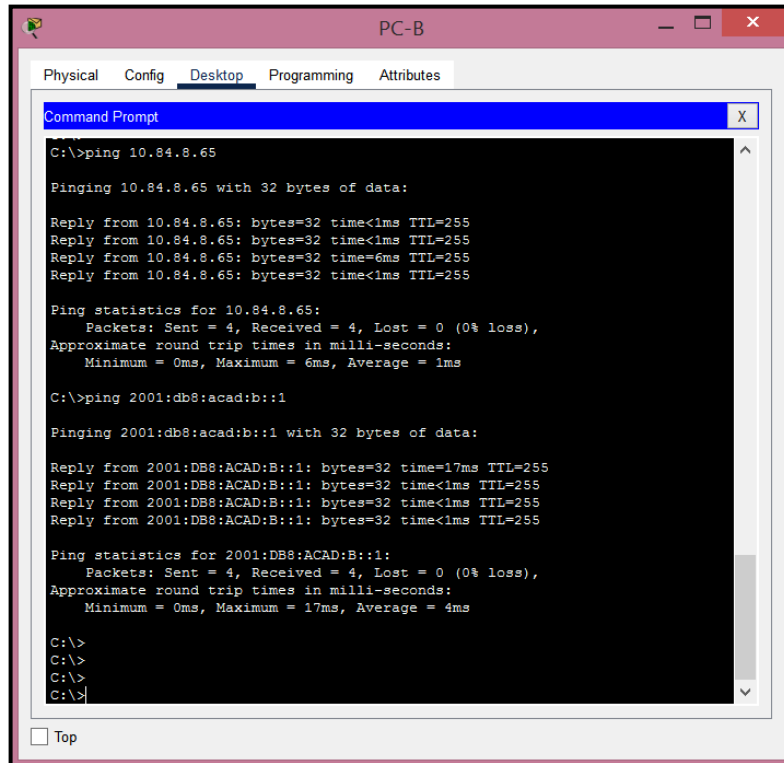


Fuente: Propia

2.10.10 Ping desde PC-B a R1 G0/0/1.30 IPv4 (10.84.8.65) e IPv6 (2001:db8:acad:b::1).

Se verifica la existencia de comunicación entre la PC-B y el router R1 en la interface G0/0/1.30, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 30 (Estudiantes), así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 26. Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.30

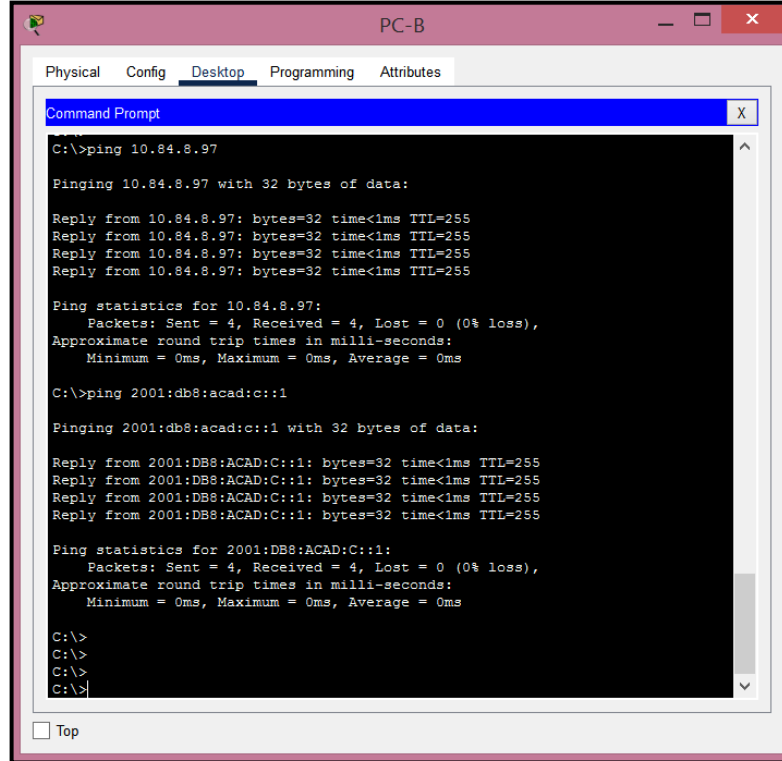


Fuente: Propia

2.10.11 Ping desde PC-B a R1 G0/0/1.40 IPv4 (10.84.8.97) e IPv6 (2001:db8:acad:c::1)

Se verifica la existencia de comunicación entre la PC-B y el router R1 en la interface G0/0/1.40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados), así mismo se comprueba que los dos hosts se comunican dentro de las dos subredes tanto para el protocolo IPv4 como el IPv6, como consecuencia de la configuración de SDM en el switch para que admita IPv6, entre otras configuraciones dentro del router como habilitar el routing IPv6.

Figura 27 Verificación comunicación IPv4 e IPv6 desde PC-B a G0/0/1.40



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.84.8.97

Pinging 10.84.8.97 with 32 bytes of data:

Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255
Reply from 10.84.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.84.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:c::1

Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:C::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

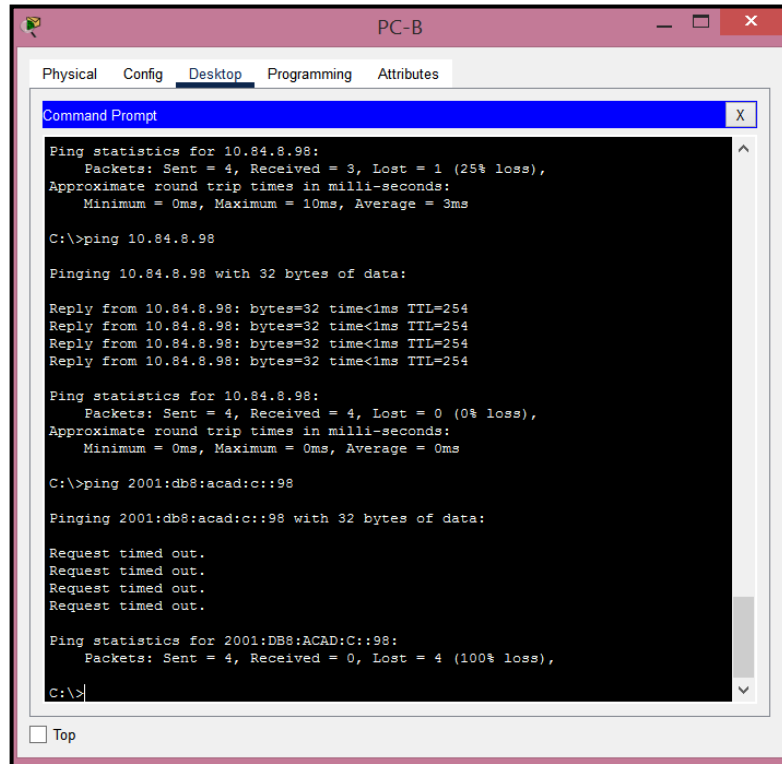
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

2.10.12 Ping desde PC-B a S1 VLAN40 IPv4 (10.84.8.98) e IPv6 (2001:db8:acad:c::98)

Se verifica la existencia de comunicación entre la PC-B y el switch S1 en la interface VLAN40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados) para IPv4. Para IPv6 no hay conexión debido a una limitación del IOS del simulador.

Figura 28. Verificación comunicación IPv4 e IPv6 desde PC-B a S1 VLAN-40



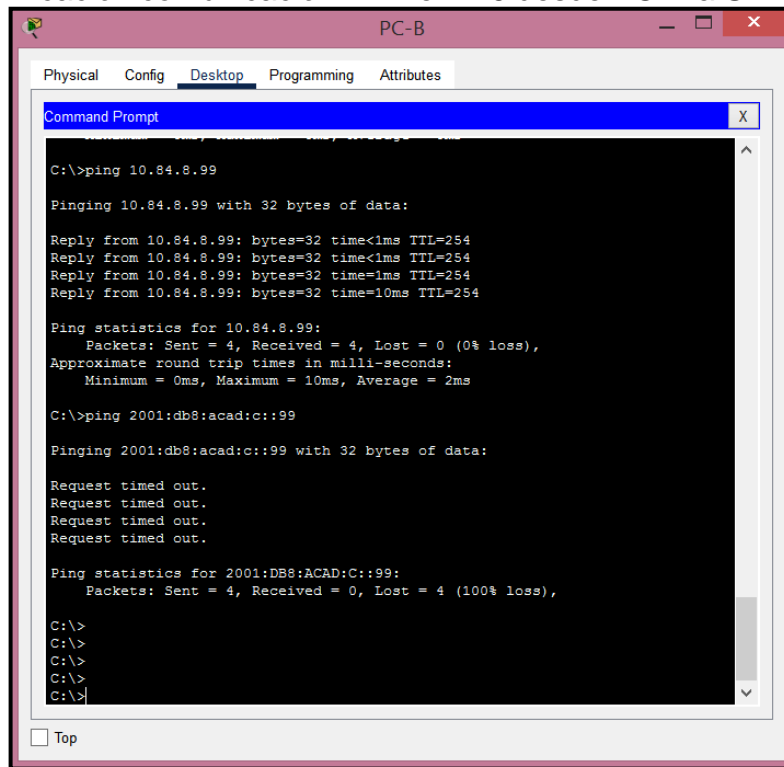
```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 10.84.8.98:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms
C:\>ping 10.84.8.98
Pinging 10.84.8.98 with 32 bytes of data:
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Ping statistics for 10.84.8.98:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db8:acad:c::98
Pinging 2001:db8:acad:c::98 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB8:ACAD:C::98:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Fuente: Propia

2.10.13 Ping desde PC-B a S2 VLAN40 IPv4 (10.84.8.99) e IPv6 (2001:db8:acad:c::99)

Se verifica la existencia de comunicación entre la PC-B y el switch S2 en la interface VLAN40, lo cual obedece a la correcta configuración de las direcciones IP, la puerta de enlace, la VLAN 40 (Invitados) para IPv4. Para IPv6 no hay conexión debido a una limitación del IOS del simulador.

Figura 29. Verificación comunicación IPv4 e IPv6 desde PC-B a S2 VLAN-40



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.84.8.99
Pinging 10.84.8.99 with 32 bytes of data:
Reply from 10.84.8.99: bytes=32 time<1ms TTL=254
Reply from 10.84.8.99: bytes=32 time<1ms TTL=254
Reply from 10.84.8.99: bytes=32 time=1ms TTL=254
Reply from 10.84.8.99: bytes=32 time=10ms TTL=254
Ping statistics for 10.84.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>ping 2001:db8:acad:c::99
Pinging 2001:db8:acad:c::99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
C:\>
C:\>
C:\>
C:\>
```

Fuente: Propia

CONCLUSIONES

El método de acceso SSH es un método para establecer de manera remota una conexión segura entre un cliente y un servidor; este protocolo encripta todo lo que envía y recibe a través de la interfaz virtual lo que permite tener seguridad en los datos enviados durante la conexión.

Con la realización de la práctica evidencie que uno de los requisitos para que se pueda realizar ping entre las PCs y los demás host de una subred es el configurar la dirección IP, por lo cual cada dispositivo de una red se debe configurar con las direcciones IP.

Al realizar la implementación de los ejercicios solicitados evidencie que uno de los métodos de proteger la configuración de los dispositivos es establecer contraseñas tanto en el modo usuario como en el modo administrador (privilegiado), así mismo se debe realizar el cifrado.

Al realizar el subneteo por el método de VLSM se obtienen subredes con diferentes cantidades de host logrando un mejor aprovechamiento y optimización del uso de direcciones IP.

El switch que permite con mayor facilidad al realizar una configuración dual stack en cisco es el 3560. La técnica dual-stack permite que cada dispositivo de una red coexistan con las configuración de las direcciones IP de los protocolos IPv4 al mismo tiempo con los protocolos de IPv6, comprobando que esta técnica permite que haya comunicación entre los host de la red.

La configuración de redes VLAN permite crear redes virtuales independientes dentro de una misma red física, su creación contribuyen a una mejor administración de la red porque aumenta la seguridad y rendimiento al separar los dominios de difusión.

Los enlaces troncales de VLAN aseguran que se realice el tráfico de datos entre los dispositivos que están en la misma VLAN, es decir el enlace troncal sirve de puente de comunicación y delimita a los host de una determinada VLAN de una red. Una VLAN permite crear redes independientes dentro de una misma red, mediante la configuración de los puertos de un switch o router. En una red sin VLAN

el tráfico de difusión de las tramas se envía a todos los host de toda la red, mientras que una red con VLAN cuando se envían tramas desde un host de una subred solo llegara a los puertos de switch configurados con una VLAN determinada.

BIBLIOGRAFIA

Cisco. Las redes en la actualidad. Introducción a las redes.[en línea]. [20 octubre de 2022] Disponible en: <https://contenthub.netacad.com/itn-dl/1.0.1>

Cisco. Configuración básica de Switches y terminales. [en línea]. [20 octubre de 2022] Disponible en: <https://contenthub.netacad.com/itn-dl/2.0.1>

Cisco. Configuración básica de switches y terminales. [en línea]. [20 octubre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/2.1.4>

Cisco. Protocolos y modelos. [en línea]. [20 octubre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/3.0.1>

Cisco. Capa física. [en línea]. [20 octubre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/4.0.1>

Cisco. Las redes en la actualidad. [en línea]. [20 noviembre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/5.0.1>

Cisco. Capa de enlace de datos. [en línea]. [20 noviembre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/6.0.1>

Cisco. Switching Ethernet. [en línea]. [20 noviembre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/7.0.1>

Cisco. Capa de red. [en línea]. [20 noviembre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/8.0.1>

Cisco. Resolución de dirección. [en línea]. [20 noviembre de 2022] Disponible en <https://contenthub.netacad.com/itn-dl/9.1.1>

Cisco Networking Academy. Netacad, Cisco Packet Tracer. (Versión 8.2.0.0162) [Software]. [1 septiembre 2022] Tomado de: <https://www.netacad.com/portal/resources/packet-tracer>

ANEXOS

Anexo 1:

Archivo escenario1.pkt

Anexo 2:

Archivo escenario2.pkt