

SOLUCION DE DOS ESTUDIOS DE CASOS BAJO EL USO
DE TECNOLOGIA CISCO

EDGAR ANDRES TEJADA MELO

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

SOLUCION DE DOS ESTUDIOS DE CASOS BAJO EL USO
DE TECNOLOGIA CISCO

EDGAR ANDRES TEJADA MELO

DIPLOMADO COMO OPCION DE GRADO PARA OPTAR EL TITULO
DE INGENIERIA DE SISTEMAS

PAULITA FLOR SALAZAR

DIRECTOR:

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Pasto, 5 de diciembre del 2022

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN	9
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO.....	11
Descripción de escenarios propuestos para la prueba de habilidades	11
Escenario 1	11
Parte 1: Construya la Red	11
Parte 2: Desarrolle el esquema de direccionamiento IP	11
Parte 3: Configure aspectos básicos	12
Paso 1: configurar los ajustes básicos.....	12
Configuración de router 1	12
Paso 2. Configuras los equipos	16
Configuración de red PC_A.....	16
Configuración de red PC_A.....	17
Escenario 2	22
Topología de escenario 2.....	22
Parte 1: Inicializar y Recargar, y configurase aspectos básicos de los dispositivos	24
Paso 1: Inicializar y volver a cargar el router y el switch.....	24
Paso 2: configurar R!	25
Paso 3: Configure S1	28
3.1 Las tareas de configuración S2.....	30
Parte 2: configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)....	32
Paso 4: configurar S1.....	32
Paso 5: Configure el S2	34
Parte 2: Configuras soporte de host	36
Paso 1: Configure R1.....	36
Paso 2: configurase los servidores.....	37
Parte 3: Probar y verificar la conectividad de extremo a extremo.....	38

Pruebas para conectividad IPv4 e IPv6 en la red.....	40
CONCLUSIONES	48
BIBLIOGRAFÍA	49
LISTAS DE ANEXOS.....	51

LISTA DE TABLAS

Tabla 1 de direccionamiento 1.	12
Tabla 2 configuración de Router 1	13
Tabla 3 configuración de Switch 1	16
Tabla 4 Configuración de PC-A	17
Tabla 5 configuración de PC-B	18
Tabla 6 Conectividad de red	18
Tabla 7 VLAN	23
Tabla 8 Asignación de direcciones	24
Tabla 9 Recarga de inicialización Router	22
Tabla 10 Recarga de inicialización Switch	25
Tabla 11 Recarga de inicialización Switch 2	25
Tabla 12 Recarga de inicialización Router 1	27
Tabla 13 configuración Switch 1	30
Tabla 14 configuración Switch 2	32
Tabla 15 configuración VLAN Switch 1	34
Tabla 16 configuración VLAN Switch 2	36
Tabla 17 configuración Router 1 Tareas	37
Tabla 18 configuración de red PC-A	38
Tabla 19 configuración de red PC-B	39
Tabla 20 Verificación de dispositivos de red - Escenario 2	39

LISTA DE FIGURAS

Figuras 1. Topología escenario 1	12
Figuras 2. Ping PC-A interface g0/0/0	19
Figuras 3. Ping PC-A interface g0/0/1	20
Figuras 4. Ping PC-A interface VLAN 1	20
Figuras 5. Ping PC-A interface VLAN 1	21
Figuras 6. Ping PC-B interface g0/0/0	21
Figuras 7. Ping PC-B interface g0/0/1	22
Figuras 8. Ping PC-B interface VLAN	22
Figuras 9. Topología escenario 2	22
Figuras 10. Configuración router tareas	40
Figuras 11. Conexión de topología escenario 2	41
Figuras 12. Ping PC-A R1 IPV4- IPV6 interfaz g0/0/1.20	41
Figuras 13. Ping PC-A R1 IPV4- IPV6 interfaz g0/0/1.30	42
Figuras 14. Ping PC-A R1 IPV4- IPV6 interfaz g0/0/1.30	42
Figuras 15. Ping PC-A R1 IPV4- IPV6 interfaz VLAN40	43
Figuras 16. Ping PC-A R1 IPV4- IPV6 interfaz VLAN40	43
Figuras 17. Ping PC-A R1 IPV4- IPV6 interfaz PC-B	44
Figuras 18. Ping PC-A R1 IPV4- IPV6 interfaz PC-B	44
Figuras 19. Ping PC-B R1 IPV4- IPV6 interfaz R1 BUCLE 0	45
Figuras 20. Ping PC-B R1 IPV4- IPV6 interfaz R1 BUCLE 0	45
Figuras 21. Ping PC-B R1 IPV4- IPV6 interfaz g0/0/1.20	44
Figuras 22. Ping PC-B R1 IPV4- IPV6 interfaz g0/0/1.30	47
Figuras 23. Ping PC-B R1 IPV4- IPV6 interfaz g0/0/1.40	47
Figuras 24. Ping PC-B R1 IPV4- IPV6 interfaz S 1 VLAN	48
Figuras 25. Ping PC-B R1 IPV4- IPV6 interfaz S2 VLAN	48

GLOSARIO

¹DHCP (Protocolo de configuración dinámica de host): Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

Ethernet: Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

ENLACE TRONCAL: Enlace que se configura en uno o varios puertos de un switch, que permite el tráfico de varias VLANs configuradas. Perteneció al estándar IEEE 802.1Q

LOOPBACK: Interfaz de red virtual que prueba el funcionamiento de transmisión de datos y conectividad.

Gateway: Dispositivo de una red que sirve como punto de acceso a otra red. El Gateway predeterminado es utilizado por un host cuando la dirección de destino de un paquete IP pertenece a algún lugar fuera de la subred local. Un router es un buen ejemplo de un Gateway predeterminado.

Router: Enrutador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

WLAN (Wireless Local Area Network): Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica.

¹ VILLALTA, Pedro, Cisco Glosario Sobre Redes de Computadoras, 2011

RESUMEN

La experiencia de escenarios, hace parte del diplomado de profundización Cisco CCNP, el cual evalúa algunos conceptos de aprendizaje a través de los módulos educativos, orientado al análisis y solución de problemas, que se puedan presentar en una red determinada. La metodología de trabajo práctico, está combinado por dos escenarios diseñados y montados, en la herramienta que ofrece Cisco System, Packet Tracer, para las configuraciones básicas de seguridad, edificación de conexión, enrutamiento y de comunicación, para las redes conmutadas. Las redes agrupan distintos puntos de conexión como router, switch, PC y servidores, acoplados por medio de cable de cobre directo, cable de cobre cruzado y cable serial DCE, según la topología y que dentro de la configuración básica admita conectividad IPv4 e IPv6, entre VLAN, DHCP, OSPF Etherchannel y port- security.

Palabras Clave: CISCO, CCNA, Conmutadas, Enrutamiento, Redes, vlan, dhcp

ABSTRACT

The scenario experience is part of the Cisco CCNP deepening diploma, which evaluates some learning concepts through educational modules, oriented to the analysis and solution of problems that may occur in a given network. The practical work methodology is combined by two scenarios designed and assembled, in the tool offered by the Cisco System, Packet Tracer, for basic security configurations, connection building, routing and communication, for switched networks. The networks group different connection points such as router, switch, PC and servers, coupled by means of direct copper cable, crossed copper cable and DCE serial cable, depending on the topology and that within the basic configuration supports IPv4 and IPv6 connectivity, between VLAN, DHCP, OSPF Etherchannel and port-security.

Keywords: CISCO, CCNA, Switched, Routing, Networking, VLANs, dhcp

INTRODUCCIÓN

Los métodos para realizar esta evaluación se presenta dos escenarios, donde se desarrolla las pruebas de conocimientos prácticas CCNA, en el simulador de cisco Packet Tracer aplicando conocimientos y habilidades adquiridas en el transcurso del diplomado de profundización de CISCO, tratando temas de , configuración fundamental de dispositivos para ser administrados y direccionados en IPv4 e IPv6, como es el caso de VLAN, protocolo de enlace troncal, protocolos de tiempo de red, servidores DHCP, Network Address Translation (NAT), listas de control de acceso, encapsulamiento por 802.1q, entre otros.

Se establecieron niveles de seguridad para la protección de los dispositivos de la red, como routers y switches, aún más, cuando alguien intenta ingresar sin permiso o ante un posible ataque; entre las medidas se encuentran, el servicio de encriptación de contraseñas, contraseñas cifradas para el modo EXEC privilegiado, contraseña de consola, deshabilitar puertos no utilizados.

En las configuraciones básicas de los dispositivos de redes, es importante la creación de usuarios administrativos locales y remotos, en donde las conexiones del protocolo SSH son totalmente cifradas y la información viaja a través de un canal seguro, generando una clave criptográfica RSA con un módulo de 1024 bits,

DESARROLLO

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

En la topología del escenario 1 se utilizó un router Cisco ISR 4321, 1 switches Cisco 2960 2 (dos) PC, como medio de conexión se utilizó, cable serial DCE, cable de cobre directo y cable de cobre cruzado, con el fin de configurar una pequeña red segura, que además admita conectividad IPv4.

Parte 1: Construya la Red

Figuras 1: Topología 1



Fuente: Prueba de habilidades diplomado CCNA

Parte 2: Desarrolle el esquema de direccionamiento IP

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

Tabla de asignación de direcciones

Tabla 1. direccionamiento

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

Autor: Prueba de habilidades diplomado CCNA

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguiente

Configuración de router 1

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando `no ip domain-lookup` y así evitar que intente traducir comandos mal ingresados. Es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando `hostname`, seguido de R1 nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio `ccna-sa.com` con el uso del comando `ip domain-name`.

Se crear una contraseña de acceso al modo privilegiado con el comando `enable`

secret "ciscoenpass" y otra de acceso por consola con password "ciscoconpass" habilitando con login el inicio de sesión. También se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando transport input ssh, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando service password-encryption. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando banner motd, con un mensaje '#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #

Cuando se configurar la interfaz del router G0/0/1, G0/0/0, donde se les asignará una descripción, una dirección IPv4 para el buen funcionamiento del protocolo, al finalizar se ingresa el comando no shutdown, el cual habilita las interfaces., por otro lado, escribiendo el comando crypto key generate rsa se genera una clave criptográfica RSA con un módulo de 1024 bits.

Tabla 2. configuración Router 1

Tarea	Especificación
Desactivar la búsqueda DNS	ROUTER(config)#no ip domain lookup
Nombre del router	ROUTER(config)#hostname R1
Nombre de dominio	R1 (config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login S2(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)# security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass

Configure 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
configurase las líneas VTY para que acepten únicamente las conexiones SSH	R1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un banner MOTD	R1 (config)# banner motd #R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #.
configuración de interface G0/0/0	R1(config)#interface g0/0/ 1 R1(config-subif)#ip address 172.77.3.62 255.255.255.192 R1(config-if)#no shutdown
configuración de interface G0/0/1	R1(config)#interface g0/0/0 R1(config-subif)#ip address 172.77.3.94 255.255.255.224 R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R2(config)#crypto key generate rsa

Autor: Prueba de habilidades diplomado CCNA y Propia

Configuración de S1 incluyen lo siguiente:

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando `no ip domain-lookup` y así evitar que intente traducir comandos mal ingresados. Es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando `hostname`, seguido de S1 nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio `ccna-sa.com` con el uso del comando `ip domain-name`.

Se crear una contraseña de acceso al modo privilegiado con el comando `enable secret "ciscoenpass"` y otra de acceso por consola con `password "ciscoconpass"` habilitando con `login` el inicio de sesión. También se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al

router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando `transport input ssh`, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando `service password-encryption`. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando `banner motd`, con un mensaje `'#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #`

Como ya se cuenta con acceso al sistema, se ingresa el comando *config terminal*, en este punto del proceso, se da inicio a la creación de las VLANs mediante el comando *vlan* (número de la vlan) y *name* seguido del nombre que se la va a asignar.

Las tareas de configuración S1

Tabla 3. configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Apagar todos los puertos sin usar	S1(config)# int range f0/1-4,f0/7-24, f0/2 S1(config-if-range)# shutdown
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local

ConFigurasr las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
ConFigurasr un banner MOTD	S1 (config)# banner motd #R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #
	S2(config)#interface vlan 1 S2(config-if)#ip address 172.77.3.2 255.255.255.192 S2(config-if)#no shutdown S2(config-if)#exit

Autor: Prueba de habilidades diplomado CCNA y Propia

Paso 2. Configuras los equipos

El equipo host PC-A, a continuación, se configurar cada servidor, registre las configuraciones de red del host

Configuración de red PC_A

Tabla 4: configuración PC-A

configuración de red de PC-A	
Descripción	Ipv4 address static
Dirección física	FE80::2E0:8FFF:FEE0:95C
Dirección IPv4	172.77.3.11
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.77.3.62

Autor: Prueba de habilidades diplomado CCNA y Propia

El equipo host PC-B, a continuación, se configurará cada servidor, registre las configuraciones de red del host

Configuración de red PC_A

Tabla 5: configuración PC-B

configuración de red de PC-B	
Descripción	Ipv4 address static
Dirección física	FE80::20A:41FF:FE5D:BDA8
Dirección IPv4	172.77.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.77.3.94

Autor: Prueba de habilidades diplomado CCNA y Propia

Parte 4: Probar y verificar la conectividad de extremo a extremo

Utilizando la siguiente tabla se verificará metódicamente la conectividad con cada dispositivo de red.

Conectividad de extremo a extremo PC-A , PC-B

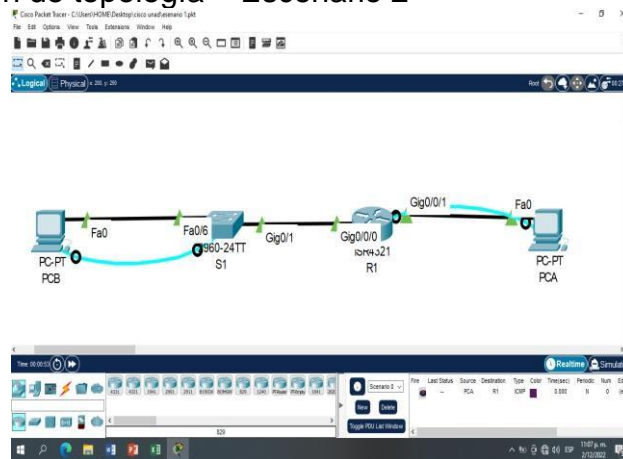
Tabla 6: Conectividad de red

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.77.3.94	SUCCESSFUL
	R1 G0/0/1	172.77.3.62	SUCCESSFUL
	S1 VLAN 1	172.77.3.2	SUCCESSFUL
	PC-B	172.17.3.75	SUCCESSFUL
PC-B	R1 G0/0/0	172.77.3.94	SUCCESSFUL
	R1 G0/0/1	172.77.3.62	SUCCESSFUL
	S1 VLAN1	172.77.3.2	SUCCESSFUL

Autor: Prueba de habilidades diplomado CCNA y Propia

En la topología de escenario 1 se puede observar el correcto funcionamiento de la red pequeña, en equipos que admiten conectividad Ipv4 en los hosts soportados, para tener una mejor certeza de la afirmación anterior, se usara el comando *Ping* en base a la *tabla 6 con* el fin de probar la conectividad entre todos los dispositivos de la red.

Figuras 2: Conexión de topología – Escenario 2



Fuente: propia

Conectividad desde PC-A a la dirección ipv4 172.77.3.94 del router R1, interfaz G0/0/0.

Figuras 2: ping PC-A – R1 Interface G0/0/0

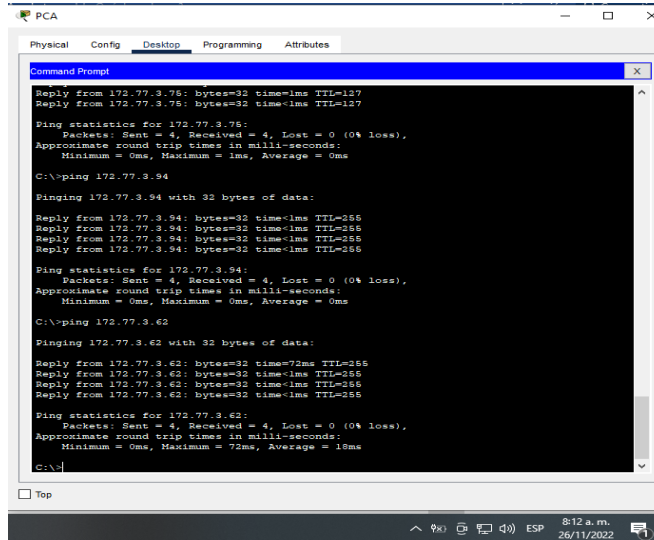
```

PCA
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.78: bytes=32 time=1ms TTL=127
Reply from 172.77.3.78: bytes=32 time=1ms TTL=127
Ping statistics for 172.77.3.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.77.3.94
Pinging 172.77.3.94 with 32 bytes of data:
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.62
Pinging 172.77.3.62 with 32 bytes of data:
Reply from 172.77.3.62: bytes=32 time=72ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 72ms, Average = 19ms
C:\>
    
```

Fuente: propia

Conectividad desde PC-A a la dirección ipv4 172.77.3.62 del router R1, interfaz G0/0/

Figuras 3: ping PC-A - R1 –G0/0/1

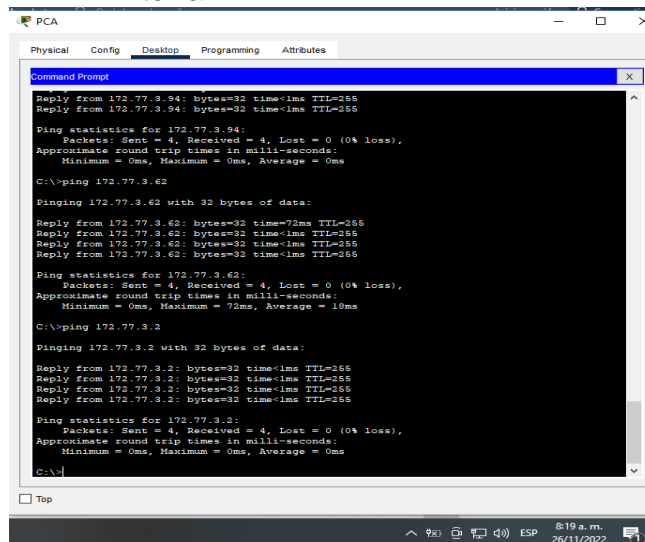


```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.75: bytes=32 time=1ms TTL=127
Reply from 172.77.3.75: bytes=32 time=1ms TTL=127
Ping statistics for 172.77.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 172.77.3.94
Pinging 172.77.3.94 with 32 bytes of data:
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.62
Pinging 172.77.3.62 with 32 bytes of data:
Reply from 172.77.3.62: bytes=32 time=72ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 72ms, Average = 18ms
C:\>
```

Fuente: propia

Conectividad desde PC-A a la dirección ipv4 172.77.3.2 del router R1, interfaz S1 VLAN

Figuras 4: ping PC- A R1 Interfaz VLAN 1



```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Reply from 172.77.3.94: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.62
Pinging 172.77.3.62 with 32 bytes of data:
Reply from 172.77.3.62: bytes=32 time=72ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 72ms, Average = 18ms
C:\>ping 172.77.3.2
Pinging 172.77.3.2 with 32 bytes of data:
Reply from 172.77.3.2: bytes=32 time=1ms TTL=255
Reply from 172.77.3.2: bytes=32 time=1ms TTL=255
Reply from 172.77.3.2: bytes=32 time=1ms TTL=255
Reply from 172.77.3.2: bytes=32 time=1ms TTL=255
Ping statistics for 172.77.3.2:
    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

Conectividad desde PC-A a la dirección ipv4 172.77.3.2 del router R1, interfaz S1 VLAN

Figuras 5: ping PC- A R1 Interfaz VLAN 1

```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255

Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 72ms, Average = 18ms

C:\>ping 172.77.3.2

Pinging 172.77.3.2 with 32 bytes of data:

Reply from 172.77.3.2: bytes=32 time<1ms TTL=255
Reply from 172.77.3.2: bytes=32 time<1ms TTL=255
Reply from 172.77.3.2: bytes=32 time<1ms TTL=255
Reply from 172.77.3.2: bytes=32 time<1ms TTL=255

Ping statistics for 172.77.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.77.3.75

Pinging 172.77.3.75 with 32 bytes of data:

Reply from 172.77.3.75: bytes=32 time<1ms TTL=127
Reply from 172.77.3.75: bytes=32 time<1ms TTL=127
Reply from 172.77.3.75: bytes=32 time<1ms TTL=127
Reply from 172.77.3.75: bytes=32 time<1ms TTL=127

Ping statistics for 172.77.3.75:
    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

Conectividad desde PC-B a la dirección ipv4 172.77.3.94 del router R1, interfaz S1 G/0/0

Figuras 6: ping PC- B R1 Interfaz G0/0/0

```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.77.3.62

Pinging 172.77.3.62 with 32 bytes of data:

Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255

Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.77.3.94

Pinging 172.77.3.94 with 32 bytes of data:

Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255

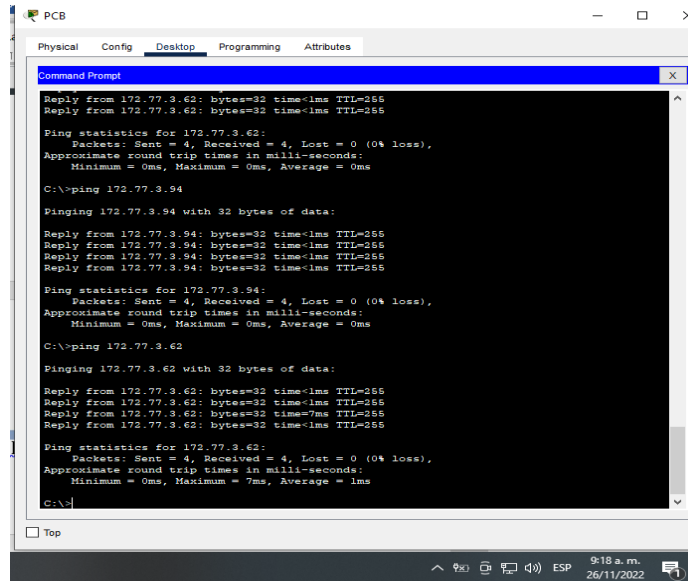
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: propia

Conectividad desde PC-B a la dirección ipv4 172.77.3.62 del router R1, interfaz S1 G/0/1

Figuras 7: ping PC- A R1 Interfaz G0/0/1

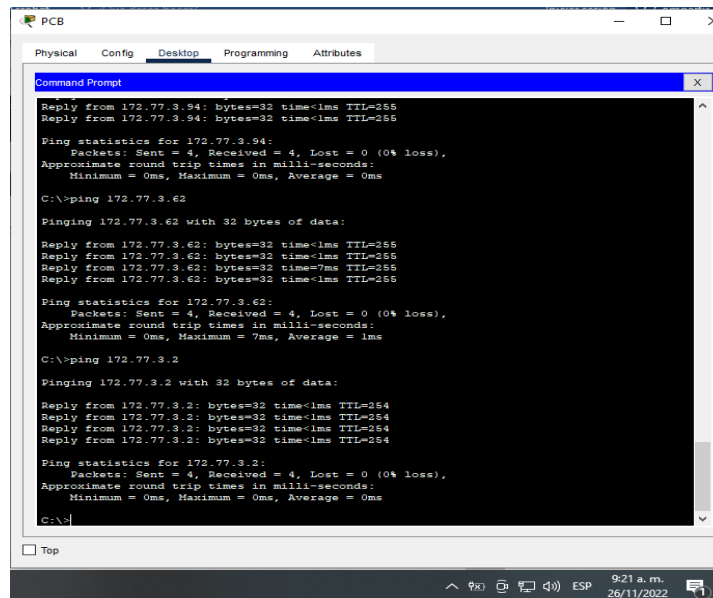


```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.94
Pinging 172.77.3.94 with 32 bytes of data:
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.62
Pinging 172.77.3.62 with 32 bytes of data:
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=7ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms
C:\>
```

Fuente: autor

Conectividad desde PC-B a la dirección ipv4 172.77.3.2 del router R1, interfaz S1 VLAN 1

Figuras 8: ping PC- B R1 Interfaz VLAN 1



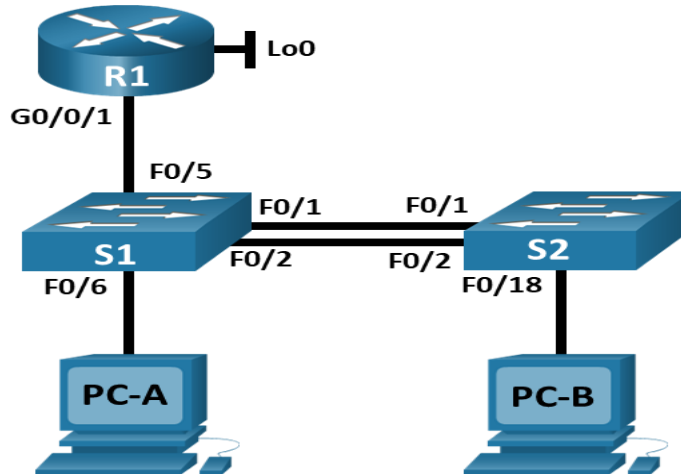
```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Reply from 172.77.3.94: bytes=32 time<1ms TTL=255
Ping statistics for 172.77.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 172.77.3.62
Pinging 172.77.3.62 with 32 bytes of data:
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Reply from 172.77.3.62: bytes=32 time=7ms TTL=255
Reply from 172.77.3.62: bytes=32 time<1ms TTL=255
Ping statistics for 172.77.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms
C:\>ping 172.77.3.2
Pinging 172.77.3.2 with 32 bytes of data:
Reply from 172.77.3.2: bytes=32 time<1ms TTL=254
Reply from 172.77.3.2: bytes=32 time<1ms TTL=254
Reply from 172.77.3.2: bytes=32 time<1ms TTL=254
Reply from 172.77.3.2: bytes=32 time<1ms TTL=254
Ping statistics for 172.77.3.2:
    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

Escenario 2

Topología de escenario 2

Figuras 9: Topología



Fuente: Prueba de habilidades diplomado CCNA

En la topología del escenario dos se manejó dos router Cisco 2960 ISS15, 2 (dos) switches de red de Cisco2960 IOS15 de 24 puertos fas ethernet, 2 gigabit ethernet y 2 (dos) PC, las conexiones se llevaron a cabo por medio de cable de cobre directo y así poder configurar una red pequeña, donde se pueda administrar de forma segura y se admita la conectividad IPv4 e IPv6..

Tabla de VLAN

Tabla 7: Vlan

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

Autor: Prueba de habilidades diplomado CCNA y Propio

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberá reemplazarlos por los últimos dos dígitos de su número de identificación.

Tabla 8: asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.XY.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.XY.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.XY.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.XY.8.98 /29	10.XY.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.XY.8.99 /29	10.XY.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

Autor: Prueba de habilidades diplomado CCNA y Propia

Parte 1: Inicializar y Recargar, y configurase aspectos básicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

Ingresamos modo EXEC privilegiado del router R1 y se escribe el comando erase startup-config, el cual borra todas las configuraciones iniciales y aparecerá un mensaje de aviso que informara si se desea borrar todos los archivos de configuración del sistema, confirmamos con la tecla ENTER, luego se aplica el comando reload, el cual reinicia manualmente el router, el proceso tardara unos cuantos segundos, y va a aparecer un diálogo de configuración del sistema, escribimos las letras no.

Tabla 9: Recarga de inicialización ROUTER

Tarea	Comando de IOS
Ingresar modo privilegiado del router	Router>enable
Eliminar configuración inicial	Router#erase startup-config
Reiniciar manualmente el router	Router#reload

Autor: Prueba de habilidades diplomado CCNA y Propia

Una vez terminado lo anterior con el router, se identifican los switches de nombre S1 y S2, posteriormente se ingresa al modo privilegiado del dispositivo, por medio del comando show flash se verifica que no se encuentren almacenados datos de VLAN en la memoria, sin embargo, se escribe el comando erase startup-config, que para confirmar el proceso a ejecutar se presiona ENTER, ahora se aplica un reiniciado manual

Tabla 10: Recarga de inicialización switch 1 y 2

Ingresar modo privilegiado del switch	Switch>enable
Verificar datos de VLAN en la memoria	Switch#show flash
Eliminar configuración anterior. Confirmar la acción a realizar.	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Reiniciar manualmente el switch	Switch#reload

Autor: Prueba de habilidades diplomado CCNA y Propia

El siguiente paso es configurar la plantilla SDM y optimizar la compatibilidad para que pueda admitir IPv4 e IPv6 los dos switches de cisco 2960 ISSo15 de 24 puertos fasethernet y dos gigabit ethernet. Se ingresa al modo privilegiado, de configuración global y se ingresa el comando sdm prefer dual-ipv4-and-ipv6 default, la palabra clave default mantiene un equilibrio de las funciones de capa 2 y capa 3; al finalizar aparece un mensaje que nos informa que la configuración del sistema ha sido modificada, y pregunta si desea guardar los cambios realizados, la respuesta es sí (yes), seguido presionar la tecla ENTER.

Tabla 11: Recarga de inicialización switch 1 y 2

Tarea	Comando de IOS
Ingresar modo privilegiado del switch	Switch>enable
Ingresar al modo de configuración global	Switch#config terminal
Plantilla que admite un equilibrio de funciones de Ipv4 e IPv6	Switch(config)#sdmprefer dual-ipv4-and-ipv6 default
Regresar al modo privilegiado	Switch(config)#end

Autor: Prueba de habilidades diplomado CCNA y Propia

Paso 2: configurar R!

Las tareas de configuración para R1 incluye las siguientes:

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando no ip domain-lookup y así evitar que intente traducir comandos mal ingresados. Es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando hostname, seguido de R1 nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio ccna-sa.com con el uso del comando ip domain-name.

Se crear una contraseña de acceso al modo privilegiado con el comando enable secret "class" y otra de acceso por consola con password "cisco" habilitando con login el inicio de sesión. También se crea en la base de datos local, un usuario y

una contraseña, que serán utilizadas al momento de conectarse al router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando `transport input ssh`, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando `service password-encryption`. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando `banner motd`, con un mensaje `#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #`

Configuración router R1 escenario 1

Tabla 12: configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)# ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption
Establecer la longitud mínima para las contraseñas	R1(config)# security passwords min-length 5
Crear un usuario administrativo en la base de datos local	R1(config)# username admin privilege 1 secret admin1pass
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
Configurar VTY solo aceptando SSH	
Configure un MOTD Banner	R1 (config)# banner motd #R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #
Habilitar el routing IPv6	R1(config)# ipv6 unicast-routing

<p>ConFigurasr interfaz G0/0/1 y subinterfaces</p>	<pre>R1(config)#interface g0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config- subif)#description vlan Docentes R1(config-subif)#ip address 10.77.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config)# interface g0/0/1.30 R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description vlan Estudiantes R1(config-subif)#ip address 10.77.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config)# interface g0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description vlan Invitados R1(config-subif)#ip address 10.77.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config)# interface g0/0/1.56 R1(config-subif)#encapsulation dot1q 56 Native R1(config-subif)#description vlan Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown</pre>
--	---

Configure el Loopback0 interface	<pre> R1(config-if)# interface loopback0 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)#description Internet R1(config-if)#exit </pre>
Generar una clave de cifrado RSA	<pre> R1(config)# crypto key generate rsa How many bits in the modulus 1024 </pre>

Autor: Prueba de habilidades diplomado CCNA y Propia

Paso 3: Configure S1.

Las tareas de configuración S1 incluyen lo siguiente:

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando `no ip domain-lookup` y así evitar que intente traducir comandos mal ingresados. Es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando `hostname`, seguido de S1 nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio `ccna-sa.com` con el uso del comando `ip domain-name`.

Se crear una contraseña de acceso al modo privilegiado con el comando `enable secret "class"` y otra de acceso por consola con `password "cisco"` habilitando con `login` el inicio de sesión. También se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando `transport input ssh`, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando `service password-encryption`. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando `banner motd`, con un mensaje `'#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #`

Tabla 13: Configuración switch 1 y 2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1 (config)# banner motd # R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS#
Generar una clave de cifrado RSA	S1(config)# crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 40 S1(config-if)#ip address 10.77.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#description vlan Invitados S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.77.8.97

Autor: Prueba de habilidades diplomado CCNA y Propia

Proseguimos con la configuración de interfaz de administración por medio del comando `interface`, una dirección IPv4 e IPv6 y una dirección de enlace local IPv6, luego se aplica el comando `no shutdown`, el cual habilita las interfaces.

Un terminal para que se comunique a través de la red, además de la dirección IP correcta, necesita la dirección gateway predeterminada, la cual es configurada con el uso del comando `ip default-gateway` seguido de la dirección IP 10.77.8.97. Con el fin de verificar la configuración realizada en el switch S1 se ejecuta el comando `show running-config`.segun tabla13.

3.1 Las tareas de configuración S2:

Las tareas de configuración S2 incluyen lo siguiente:

Se ingresa al modo EXEC privilegiado del router, se inhabilita la búsqueda DNS por medio del comando `no ip domain-lookup` y así evitar que intente traducir comandos mal ingresados. Es importante asignar un nombre a cada uno de ellos, para ello se utiliza el comando `hostname`, seguido de S2 nombre para el actual dispositivo, ahora es necesario asignar el nombre de dominio `ccna-sa.com` con el uso del comando `ip domain-name`.

Se crea una contraseña de acceso al modo privilegiado con el comando `enable secret "class"` y otra de acceso por consola con `password "cisco"` habilitando con `login` el inicio de sesión. También se crea en la base de datos local, un usuario y una contraseña, que serán utilizadas al momento de conectarse al router a través de SSH, pero que no permita conexiones Telnet, para ello se utiliza el comando `transport input ssh`, al finalizar es necesario encriptar todas las contraseñas que se han creado y las futuras, por medio del comando `service password-encryption`. Cuando una persona intenta acceder al router es importante crear un banner por medio del comando `banner motd`, con un mensaje `'#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS #`

Tabla 14: configuración switch 2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret class
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1 (config)# banner motd #R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus 1024
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 40 S2(config-if)#ip address 10.77.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#description vlan Management S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.77.8.97

Autor: Prueba de habilidades diplomado CCNA y Propia

Proseguimos con la configuración de interfaz de administración por medio del comando `interface`, una dirección IPv4 e IPv6 y una dirección de enlace local IPv6, luego se aplica el comando `no shutdown`, el cual habilita las interfaces.

Un terminal para que se comuniquen a través de la red, además de la dirección IP correcta, necesita la dirección gateway predeterminada, la cual es configurada con el uso del comando `ip default-gateway` seguido de la dirección IP 10.77.8.97. Con el fin de verificar la configuración realizada en el switch S1 se ejecuta el comando `show running-config`.segun table 14.

Parte 2: configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: configurar S1

La configuración del S1 incluye las siguientes tareas:

`#R1 EDGAR ANDRES TEJADA MELO INGENIRIA DE SISTEMAS#` Para dar inicio con la configuración de la infraestructura de red del switch S1, es necesario ingresar la contraseña de acceso `class`, se le indica que se desea ingresar al modo EXEC privilegiado escribiendo el comando `enable`, aquí solicita la contraseña `cisco`. Como ya se cuenta con acceso al sistema, se ingresa el comando `config terminal`, en este punto del proceso, se da inicio a la creación de las VLANs mediante el comando `vlan` (número de la vlan) y `name` seguido del nombre que se la va a asignar.

Se mira la interface a configurar y por medio el protocolo 802.1Q se agrega una etiqueta a cada trama con el ID de la VLAN que en este caso hace referencia al comando `switchport trunk native vlan 56`, que a su vez es canalizado por los puertos Trunk, que funciona como enlace entre el switch S1 y S2, para las interfaces F0/1, F0/2 y F0/5.

El EtherChannel en el switch S1, se usa el comando `channel-group 1 mode`

active, habilitando el enlace troncal del puerto e ingresando la encapsulación troncal 802.1Q, que hace referencia al comando *dot1q*, después para cambiar el Vlan nativo, se ingresa el comando *switchport trunk native vlan 56*. Ahora se configura el puerto de acceso de host para Vlan 20, llamando a la interface *Fa0/6*, acceso con el comando *switchport acces vlan 20*. Por otro lado, para configurar un número máximo de 4 direcciones, se utiliza el comando *switchport port-security maximum 4*. Finalmente se seleccionan las interfaces que no se van a utilizar, se establece el modo de acceso, se les asigna la Vlan 50, se les agrega una descripción y se apagan.

Tabla 15: configuración VLAN Switch 1

Tarea	Especificación
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	<pre> S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit </pre>
Crear troncos 802.1Q que utilicen la VLAN 56 nativa Interfaces F0/1, F0/2 y F0/5	<pre> S1(config)#interface range fa0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56 S1(config-if-range)#exit S1(config)#interface range fa0/5 S1(config-if)#switchport trunk encapsulation dot1q </pre>

	<pre>S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if-range)#shutdown</pre>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre>S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56</pre>
<p>Configurar el puerto de acceso de host para VLAN 20 Interface F0/6</p>	<pre>S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20</pre>
<p>Configurar la seguridad del puerto en los puertos de acceso</p>	<pre>S1(config-if)#switchport port-security maximum 4</pre>
<p>Proteja todas las interfaces no utilizadas</p>	<pre>S1(config-if)#interface range fa0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No utilizadas S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No utilizadas S1(config-if-range)#shutdown</pre>

Autor: Prueba de habilidades diplomado CCNA y Propia

Paso 5: Configure el S2.

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

Para la configuración del S2, es el mismo del S1, se ingresa por modo EXEC

privilegiado, se crean las VLAN, se utiliza el protocolo 802.1Q, pero a diferencia del switch S1, solo se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces *fa0/1* y *fa0/2*, de igual manera para este caso se configura el puerto de acceso del host para la VLAN 30 con la interface *fa0/18*, así mismo se configura la seguridad de los puertos y se aseguran las interfaces no utilizadas

Tabla 16: configuración VLAN Switch 2

Tarea	Especificación
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	<pre>S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit</pre>
Crear troncos 802.1Q que utilicen la VLAN 56 nativa Interfaces F0/1 y F0/2	<pre>S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56</pre>
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	<pre>S2(config-if-range)#channel-group 2 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 56</pre>
ConFigurasr el puerto de acceso del host para la VLAN 30 Interfaz F0/18	<pre>S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30</pre>

Configure port-security en los access ports	S2(config-if)#switchport port-security maximum 4
Asegure todas las interfaces no utilizadas.	S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No utilizadas S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No utilizadas S2(config-if-range)#shutdown

Autor: Prueba de habilidades diplomado CCNA y Propia

Parte 2: Configuras soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Se configura la puerta de enlace como última alternativa en un enrutador, esto se realiza por medio del comando `ip route 0.0.0.0 0.0.0.0` creando rutas para direccionamiento IPv4 e IPv6 que dirija el tráfico hacia la interface `loopback 0`.

Mediante el comando `ip dhcp excluded-address` se define las direcciones excluidas no asignadas, dando el rango de una IP de inicio y una IP final para el grupo VLAN 20 compuesto por las 10 direcciones de la subred solamente. Luego se pone el nombre del rango del servicio por medio del comando `ip dhcp pool`, en la siguiente línea se define la red que se encargara de dar servicio DHCP, su respectiva puerta de enlace y por último el nombre del dominio `ccna-sa.net`, el anterior procedimiento se repite para el grupo VLAN 30 con las mismas 10 direcciones con nombre de dominio que sería `ccna-sb.net`.

Tabla 17: configuración Router 1- Tareas

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0

ConFigurasr IPv4 DHCP para VLAN 20	R1(config)#ip dhcp excluded-address 10.77.8.1 10.77.8.52 R1(config)#ip dhcp pool vlan20-Estudiantes R1(dhcp-config)#network 10.77.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.77.8.1 R1(dhcp-config)#domain-name ccna-sa.net R1(dhcp-config)#exit
ConFigurasr DHCP IPv4 para VLAN 30	R1(config)#ip dhcp excluded-address 10.77.8.65 10.77.8.84 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config)#network 10.77.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.77.8.65 R1(dhcp-config)#domain-name ccna-sb.net R1(dhcp-config)#exit

Autor: Prueba de habilidades diplomado CCNA y Propia

Paso 2: configurase los servidores

El equipo host PC-A, a continuación, se configurar cada servidor, registre las configuraciones de red del host

Tabla 18: configuración de red PC-A

configuración de red de PC-A	
Descripción	Datos por DHCP
Dirección física	FE80::207:ECFF:FEEE:7654
Dirección IP	10.77.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Autor: Prueba de habilidades diplomado CCNA y Propia

El equipo host PC-A, a continuación, se configurar cada servidor, registre las configuraciones de red del host

Tabla 19: configuración de red PC-B

configuración de red de PC-B	
Descripción	Datos por DHCP
Dirección física	FE80::2E0:A3FF:FE5B:D456
Dirección IP	10.77.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.77.8.65
Gateway predeterminado IPv6	FE80::1

Autor: Prueba de habilidades diplomado CCNA y Propia

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

Utilizando la siguiente tabla se verificar metódicamente la conectividad con cada dispositivo de red.

Tabla 20: Verificación de dispositivos de red Escenario 2

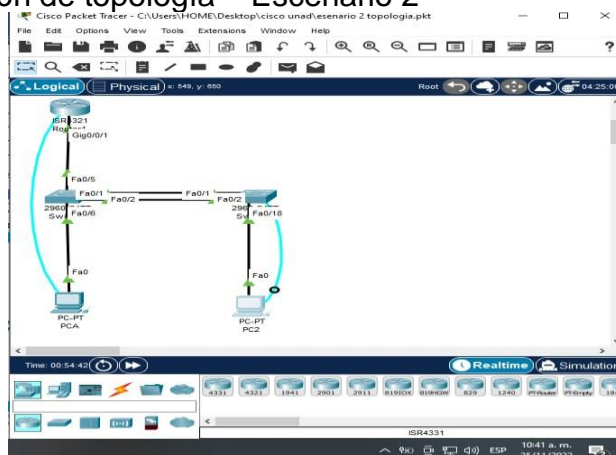
Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.77.8.1	SUCCESSFUL
		IPv6	2001:db8:acad:a::1	SUCCESSFUL
	R1, G0/0/1.30	IPv4	10.77.8.65	SUCCESSFUL
		IPv6	2001:db8:acad:b::1	SUCCESSFUL
	R1, G0/0/1.40	IPv4	10.77.8.97	SUCCESSFUL
		IPv6	2001:db8:acad:c::1	SUCCESSFUL
S1, VLAN 40		IPv4	10.77.8.98	SUCCESSFUL
		IPv6	2001:db8:acad:c::98	RECEIVED
S2, VLAN 40		IPv4	10.77.8.99	SUCCESSFUL
		IPv6	2001:db8:acad:c::99	RECEIVED
PC-B		IPv4	10.77.8.85	SUCCESSFUL
		IPv6	2001:db8:acad:b::50	SUCCESSFUL
R1 Bucle 0		IPv4	209.165.201.1	SUCCESSFUL

PC-B		IPv6	2001:db8:acad:209: :1	SUCCESSFUL
	R1 Bucle 0	IPv4	209.165.201.1	SUCCESSFUL
		IPv6	2001:db8:acad:209: :1	SUCCESSFUL
	R1, G0/0/1.20	IPv4	10.77.8.1	SUCCESSFUL
		IPv6	2001:db8:acad:a::1	SUCCESSFUL
	R1, G0/0/1.30	IPv4	10.77.8.65	SUCCESSFUL
		IPv6	2001:db8:acad:b::1	SUCCESSFUL
	R1, G0/0/1.40	IPv4	10.77.8.97	SUCCESSFUL
		IPv6	2001:db8:acad:c: :1	SUCCESSFUL
	S1, VLAN 40	IPv4	10.77.8.98	SUCCESSFUL
		IPv6	2001:db8:acad:c::9 8	RECEIVED
	S2, VLAN 40	IPv4	10.77.8.99	SUCCESSFUL
	IPv6	2001:db8:acad:c::9 9	RECEIVED	

Autor: Prueba de habilidades diplomado CCNA y Propia

En la topología de escenario 2 se puede observar el correcto funcionamiento de la red pequeña, en equipos que admiten conectividad Ipv4 e IPv6 en los hosts soportados, para tener una mejor certeza de la afirmación anterior, se usara el comando *Ping* en base a la *tabla 20* con el fin de probar la conectividad entre todos los dispositivos de la red.

Figuras 10: Conexión de topología – Escenario 2

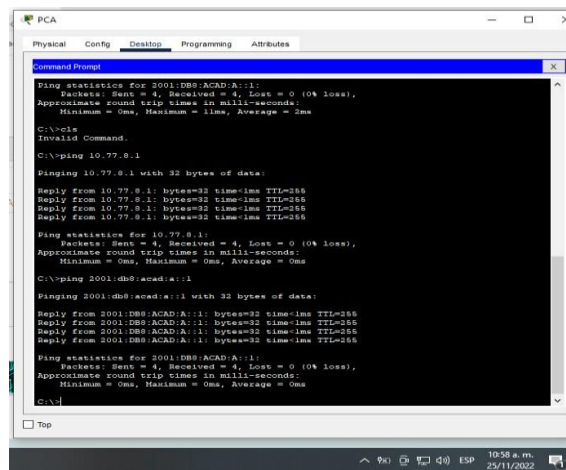


Fuente: propia

Pruebas para conectividad IPv4 e IPv6 en la red

Conectividad desde PC-A a la dirección ipv4 10.77.8.1 IPv6 2001:db8:acad:a :1 del router R1, interfaz G0/0/1.20

Figuras 11: ping PC- A R1 IPV4 IPV6 Interfaz G0/0/1.20



```
Physical Config Desktop Programming Attributes
Command Prompt

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 = 1ms, Average = 2ms

C:\>cls
Invalid Command.

C:\>ping 10.77.8.1

Pinging 10.77.8.1 with 32 bytes of data:
Reply from 10.77.8.1: bytes=32 time=1ms TTL=255
Reply from 10.77.8.1: bytes=32 time=1ms TTL=255
Reply from 10.77.8.1: bytes=32 time=1ms TTL=255
Reply from 10.77.8.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.77.8.1:
    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: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

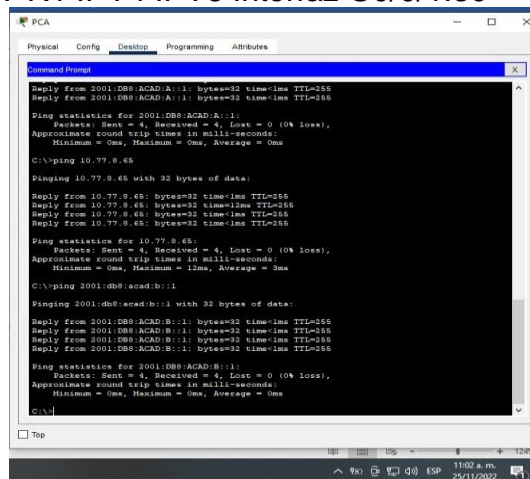
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: propia

Conectividad desde PC-A a la dirección ipv4 10.77.8.65 IPv6 2001:db8:acad:b :1 del router R1, interfaz G0/0/1.30

Figuras 12: ping PC- A R1 IPV4 IPV6 Interfaz G0/0/1.30



```
Physical Config Desktop Programming Attributes
Command Prompt

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:\>ping 10.77.8.65

Pinging 10.77.8.65 with 32 bytes of data:
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255

Ping statistics for 10.77.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 3ms

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:\>
```

Fuente: autor

Conectividad desde PC-A a la dirección ipv4 10.77.8.97 IPv6 2001:db8:acad:c :1 del router R1, interfaz G0/0/1.40

Figuras 13: ping PC- A R1 IPV4 IPV6 Interfaz G0/0/1.40

```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
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:\>ping 10.77.8.97
Pinging 10.77.8.97 with 32 bytes of data:
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Ping statistics for 10.77.8.97:
    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 = 1ms, Average = 0ms
C:\>
```

Fuente: propia

Conectividad desde PC-A a la dirección ipv4 10.77.8.98 IPv6 2001:db8:acad:c :98 del router R1, interfaz s1 VLAN40

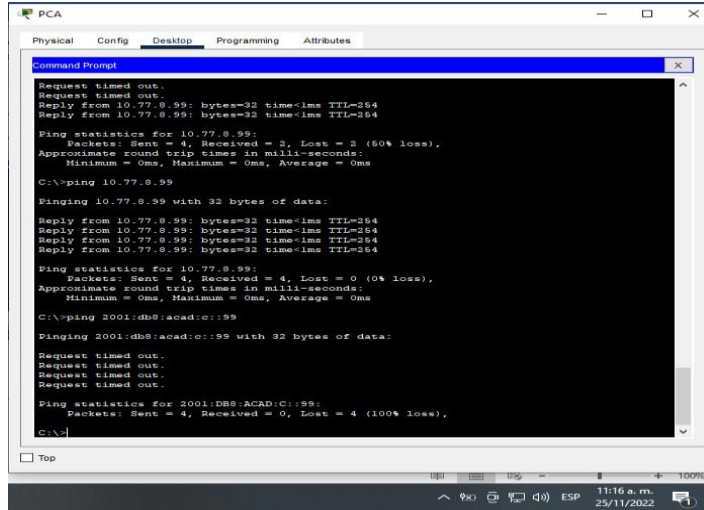
Figuras 14: ping PC- A R1 IPV4 IPV6 Interfaz VLAN.40

```
PCA
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Ping statistics for 10.77.8.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.77.8.98
Pinging 10.77.8.98 with 32 bytes of data:
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Ping statistics for 10.77.8.98:
    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

Conectividad desde PC-A a la dirección ipv4 10.77.8.99 IPv6 2001:db8:acad:c :99 del router R1, interfaz s1 VLAN40

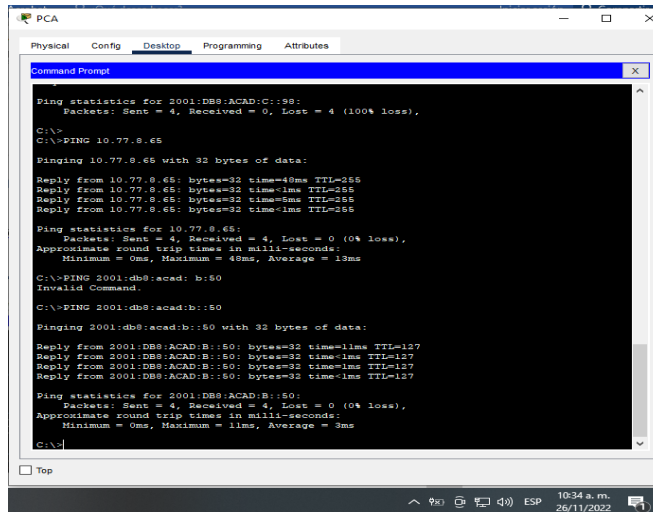
Figuras 15: ping PC- A R1 IPV4 IPV6 Interfaz VLAN40



Fuente: propia

Conectividad desde PC-A a la dirección ipv4 10.77.8.65 IPv6 2001:db8:acad:B :50 del router R1, interfaz s1 PC-B

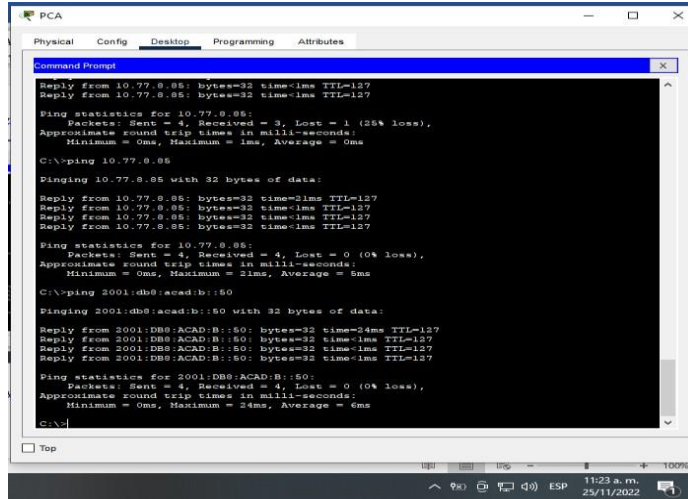
Figuras 16: ping PC- A R1 IPV4 IPV6 Interfaz PC-B



Fuente: autor

Conectividad desde PC-A a la dirección ipv4 10.77.8.53 IPv6 2001:db8:acad:b:
:50 del router R1, interfaz s1 PC-B-NIC

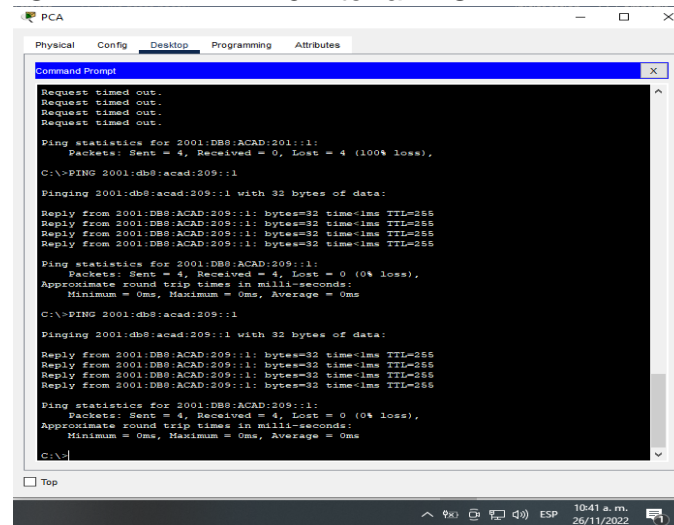
Figuras 17: ping PC- A R1 IPV4 IPV6 Interfaz PC-B



Fuente: propia

Conectividad desde PC-A a la dirección ipv4 209.165.201.1 IPv6 2001:db8:acad:b:
:209:1 del router R1, interfaz s1 PC-B-NIC

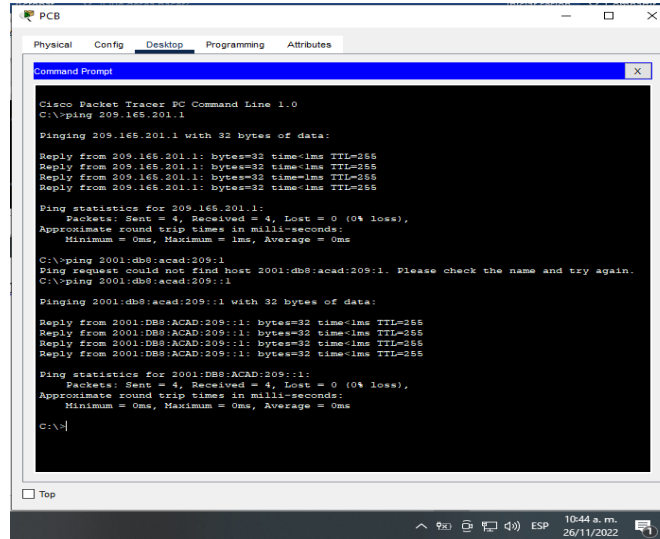
Figuras 18: ping PC- A R1 IPV4 IPV6 Interfaz PC.B



Fuente: autor

Conectividad desde PC-b a la dirección ipv4 209.165.201.1 IPv6 2001:db8:acad:209:1 del router R1, interfaz R1 bucle 0

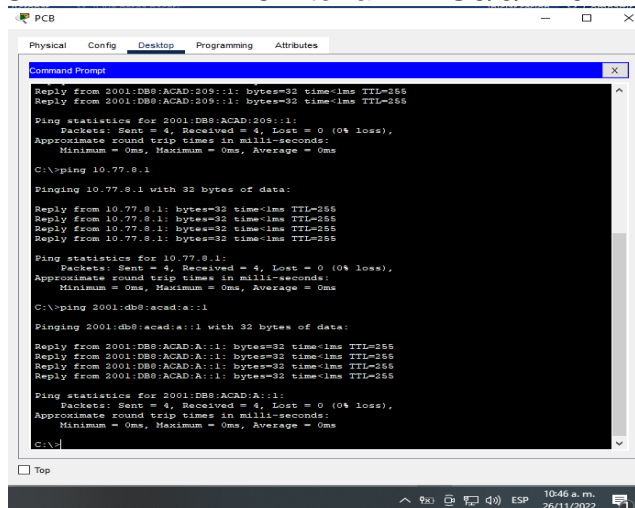
Figuras 19: ping PC-B R1 IPV4 IPV6 Interfaz R1 Bucle 0



Fuente: propia

Conectividad desde PC-B a la dirección ipv4 10.77.8.1 IPv6 2001:db8:acad:a::1 del router R1, interfaz G0/0/1.20

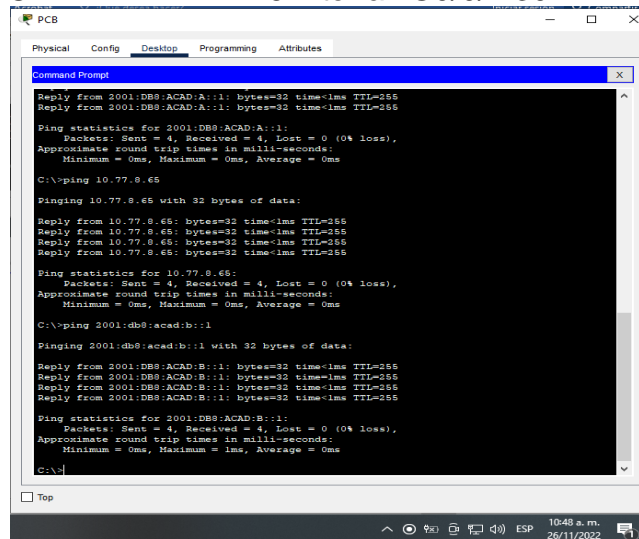
Figuras 20: ping PC-B R1 IPV4 IPV6 Interfaz R1 G0/0/1.20



Fuente: propia

Conectividad desde PC-B a la dirección ipv4 10.77.8.65 IPv6 2001:db8:acad:b::1 del router R1, interfaz G0/0/1.30

Figuras 21: ping PC- B R1 IPV4 IPV6 Interfaz G0/0/1 30

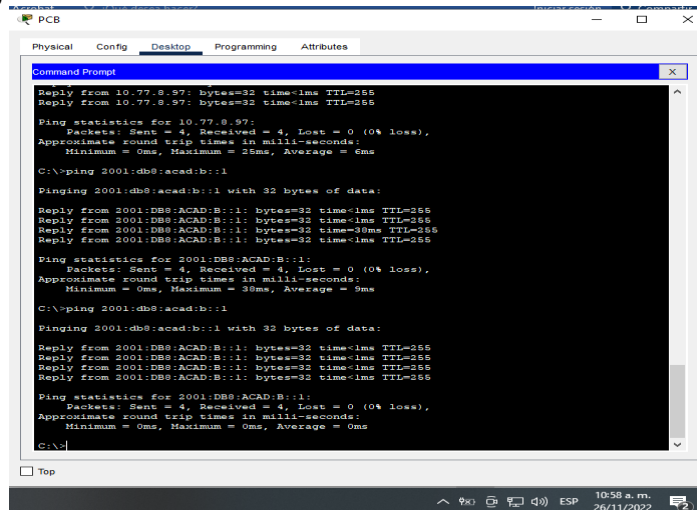


```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.77.8.65
Pinging 10.77.8.65 with 32 bytes of data:
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Reply from 10.77.8.65: bytes=32 time=1ms TTL=255
Ping statistics for 10.77.8.65:
    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: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 = 1ms, Average = 0ms
C:\>
```

Fuente: propia

Conectividad desde PC-B a la dirección ipv4 10.77.8.97 IPv6 2001:db8:acad:b::1 del router R1, interfaz G0/0/1.40

Figuras 22: ping PC- B R1 IPV4 IPV6 Interfaz G0/0/1.40

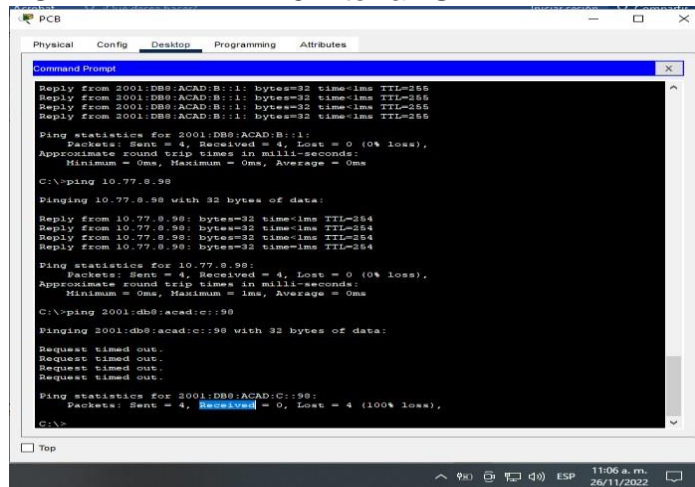


```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Reply from 10.77.8.97: bytes=32 time=1ms TTL=255
Ping statistics for 10.77.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 25ms, Average = 6ms
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=38ms 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 = 38ms, Average = 9ms
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:\>
```

Fuente: propia

Conectividad desde PC-B a la dirección ipv4 10.77.8.98 IPv6 2001:db8:acad:c::98 del router R1, interfaz s1 VLAN40

Figuras 23: ping PC- B R1 IPV4 IPV6 Interfaz S1 VLAN 4

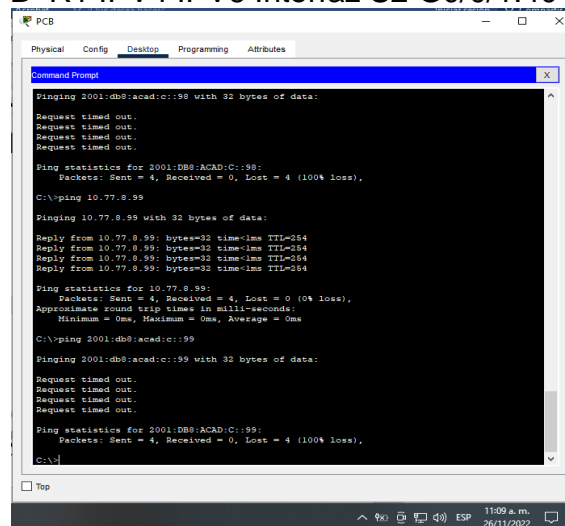


```
Command Prompt
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.77.8.98
Pinging 10.77.8.98 with 32 bytes of data:
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Reply from 10.77.8.98: bytes=32 time=1ms TTL=254
Ping statistics for 10.77.8.98:
    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::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

Conectividad desde PC-B a la dirección ipv4 10.77.8.99 IPv6 2001:db8: acad: c:99 del router R1, interfaz s2 PC-B

Figuras 24: ping PC- B R1 IPV4 IPV6 Interfaz S2 G0/0/1.40



```
Command Prompt
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:\>ping 10.77.8.99
Pinging 10.77.8.99 with 32 bytes of data:
Reply from 10.77.8.99: bytes=32 time=1ms TTL=254
Reply from 10.77.8.99: bytes=32 time=1ms TTL=254
Reply from 10.77.8.99: bytes=32 time=1ms TTL=254
Reply from 10.77.8.99: bytes=32 time=1ms TTL=254
Ping statistics for 10.77.8.99:
    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::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:\>
```

Fuente: propia

CONCLUSIONES

Por medio de estos casos de estudio se pudo poner evidenciar todo lo aprendido durante el diplomado de profundización CCNA, lo cual es de gran ayuda en la implementación de redes tanto locales como WAN.

La simulación es una gran ayuda ya que se pueden detectar las fallas y problemas en la conexión de red y se pueda verificar el funcionamiento de la red mediante los comandos ping y tracert comprendiendo los conceptos generales de enrutamiento.

Se reforzó el uso del direccionamiento Vlan en la resolución de un ejercicio de aplicación comprendiendo correctamente el uso de cableado específico para conexiones entre dispositivos

intermediarios y finales, conocido como redes LAN respectivamente, donde se repasó el papel que juegan los protocolos en el diseño de una red TCP/IP para el correcto flujo de información entre dispositivos intermedios y finales.

Se Desarrolló los esquemas IP. Para el direccionamiento IPv4 y IPv6 y se crea las redes y subredes para la cantidad requerida de hosts. Donde se Asignaron las direcciones de acuerdo con los requisitos mencionados en las tablas de direccionamiento dispositivos de red (Switch y Router) y se configuran mediante conexión de consola con comandos básicos de IOS para la configuración.

BIBLIOGRAFÍA

VILLALTA. PEDRO. Cisco Glosario Sobre Redes de Computadoras. (en Línea) (2011) 27 noviembre de 2022. Disponible en:

https://www.postecnologia.com/2013/10/glosario-redes-de-computadoras_29.html

BITACORA BYTE. Configuras DHCP en router CISCO. (en línea) (2017) 19 de noviembre de 2022), Disponible en:

<https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/>

CISCO. Configuración de una puerta de enlace de último recurso mediante comandos IP. (en línea) (2005). (27 de noviembre de 2022) Disponible en:

https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/16448-default.html

CISCO. Guía de diseño de OSPF (en línea) (2005). (20 de noviembre de 2022)

Disponible en: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>

CISCO. Información sobre los modos de loopback en routers de Cisco (en línea). (2007). (18 de noviembre de 2020), de Cisco. Disponible en:

https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-mode-atm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337-atmloopback.html

CISCO. Guía de resolución de problemas y depuración de problemas del protocolo de tiempo de red (en línea) (2013). (24 de noviembre de 2022), Disponible en:

https://www.cisco.com/c/es_mx/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html

CISCO. Verificación del estado de NTP con el comando show ntp association. (en línea) (2014) (26 de Noviembre de 2022), de Cisco:

<https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html>

CISCO. Guía de primeros pasos para el Catalyst 2960-X y Switches 2960-XR (en línea) (2020). (27 de noviembre de 2022) Disponible en:

https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst2960x/hardware/quick/guide/all_languages/b_gsg_2960xr_es_CO.pdf

LISTAS DE ANEXOS

Anexo A. Link de descarga escenario 1

https://drive.google.com/file/d/1zAKx0omVTpkobpiFmTkeSfrkOf3rJszc/view?usp=share_link

Anexo B. Link de descarga escenario 2

https://drive.google.com/file/d/1_e2nHSq7wcLU4MnAHK3cGyhgCUvFjTeh/view?usp=share_link