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

ROSA MARÍA LÓPEZ URBANO

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

BOGOTÁ
2022

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

ROSA MARÍA LÓPEZ URBANO

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

DIRECTOR:
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

BOGOTÁ, 22 de noviembre de 2022

AGRADECIMIENTOS

Le doy gracias principalmente a Dios por haberme dado salud, paciencia, fortaleza y sabiduría para que realizar el diplomado.

A mi familia que siempre me ayudo y me dio fuerzas ante las dificultades, siempre estuvieron apoyándome para poder seguir adelante.

Al equipo de tutores de la universidad que me brindaron muchos conocimientos y apoyo para lo que necesitaba y me enseñaron que todo se puede lograr con un buen trabajo, esfuerzo y dedicación.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LAN: Red de área local es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica pequeña. Normalmente, se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas. [1]

COMANDOS IOS: Permiten trabajar con los dispositivos intermediarios como Switch o Router al no tener una interfaz gráfica. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado.[2]

CIFRADO: forma de codificar los datos para evitar que individuos no autorizados vean la información en formato simple[3].

SVI: Es una interfaz virtual del Switch, se accede a esta con VLAN 1.[4]

PROTOCOLO: Reglas que permiten la comunicación. En redes, existen los protocolos de red, seguridad, routing y detección de servicios.[5]

DIRECCIÓN MAC ETHERNET: proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI. Una dirección MAC Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales.[6]

IPv4: protocolo de comunicación de la capa de red principal. Se utiliza para garantizar que el paquete se entrega en su siguiente parada en el camino a su dispositivo final de destino.[7]

---

[1] CISCO, Netacad. Introducción a las redes – LAN y WAN (2022)
[2] CISCO, Netacad. Introducción a las redes - Estructura básica de comandos de IOS (2022)
[3] CISCO, Netacad. Introducción a las redes – Encriptación de las contraseñas (2022)
[4] CISCO, Netacad. Introducción a las redes – Configuración de interfaz virtual de switch (2022)
[5] CISCO, Netacad. Introducción a las redes – Protocolos (2022)
[6] CISCO, Netacad. Introducción a las redes – Dirección MAC de Ethernet (2022)
[7] CISCO, Netacad. Introducción a las redes – Paquete IPv4 (2022)

IPv6: protocolo de comunicación de la capa de red principal que resuelve las limitaciones que se tienen con IPv4 y se adaptan a las necesidades actuales.[8]

PRUEBA DE CONECTIVIDAD: Funciones que permiten verificar la conectividad en los dispositivos de red. Por ejemplo, los comandos PING y TRACEROUTE envían solicitudes de eco a una dirección IPv4 o IPv6 para obtener una respuesta.[9]

VLAN: proporcionan la segmentación y la flexibilidad organizativa. Un grupo de dispositivos dentro de una VLAN se comunica como si cada dispositivo estuviera conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.[10]

ETHERCHANNEL: es una tecnología de agregación de enlaces que agrupa varios enlaces Ethernet físicos en un único enlace lógico. Se utiliza para proporcionar tolerancia a fallos, uso compartido de carga, mayor ancho de banda y redundancia entre switches, routers y servidores.[11]

LACP: Link Aggregation Control Protocol, permiten que los puertos con características EtherChannel formen un canal mediante una negociación dinámica con los switches adyacentes.[12]

[8] CISCO, Netacad. Introducción a las redes – Paquete IPv6 (2022)
[9] CISCO, Netacad. Introducción a las redes – Mensajes ICMP (2022)
[10] CISCO, Netacad. Conmutación, Enrutamiento y redes inalámbricas esenciales – VLANs (2022)
[11] CISCO, Netacad. Introducción a las redes – Funcionamiento de EtherChannel (2022)
[12] CISCO, Netacad. Introducción a las redes – Protocolos de negociación automática (2022)

RESUMEN

El presente informe tiene como finalidad demostrar las habilidades en la configuración de dispositivos intermedios adquiridas en los cursos CCNA1 y CCNA2 de Cisco donde se destacan ajustes de seguridad básicas, ajustes de conectividad y pruebas. De ese modo, se montan dos escenarios de simulación en la herramienta Packet Tracer y en cada una se realiza el montaje desde cero, agregando dispositivos, configurando cableado y configurando desde la consola de cada dispositivo intermedio los comandos necesarios para que se pueda realizar una correcta comunicación entre los dispositivos finales. De los resultados obtenidos se pudo observar que en los dos escenarios se cumplen con los requisitos y se evidencian mediante imágenes las pruebas de conectividad satisfactorias.

Palabras clave: red, enrutamiento, interfaz, cifrado, ping, consola, VLAN.

ABSTRACT

The purpose of this report is to demonstrate the intermediate device configuration skills acquired in Cisco's CCNA1 and CCNA2 courses that highlight basic security settings, connectivity settings, and testing. In this way, two simulation scenarios are assembled in the Packet Tracer tool and in each one the assembly is carried out from scratch, adding devices, configuring wiring, and configuring from the console of each intermediate device the necessary commands so that a correct communication between end devices. From the results obtained, it was possible to observe that in the two scenarios the requirements are met, and the satisfactory connectivity tests are evidenced by images.

Keywords: network, routing, interface, encryption, ping, console, VLAN.

INTRODUCCIÓN

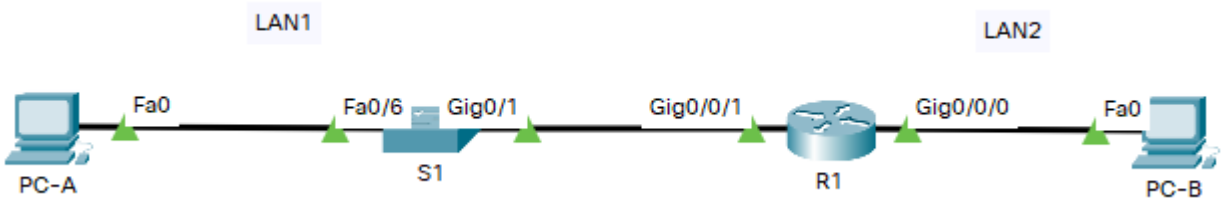
En los fundamentos de redes se describe el diseño y construcción de un cableado estructurado, se desarrollan criterios como el uso de comandos a través de consola y asignación de direcciones IP a los distintos dispositivos de red que lo componen, esto permite lograr una comunicación entre ellos.

Para la práctica de habilidades sobre lo conocimientos adquiridos, se trabajan dos escenarios con topologías distintas de red bajo el programa Packet Tracer de Cisco. El primer escenario plantea una red con dos LAN, la interacción se basa en las configuraciones básicas de un router y un switch con varias VLAN bajo IPv4.

En el segundo escenario, se van agregando criterios más complejos que incluyen direccionamiento IPv6, subinterfaces, grupos EtherChannel y DHCP habilitado desde un Router. Al final de cada escenario se detallan los resultados para validar que los ajustes empleados fueron los correctos.

1. ESCENARIO 1

Figura 1 Topología del escenario 1



Fuente: Autor

1.1. Construir la Red

En el simulador, se construye la red de acuerdo con la topología lógica planteada, se cablea conforme se indica en la topología y se conectan los equipos de cómputo.

1.2. Desarrollar esquema de direccionamiento IP

Para la dirección IPv4, se crean dos subredes con la cantidad requerida de hosts. Se asignan las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1 Definición de direccionamiento IP

Ítem	Requerimiento	Resultado
Dirección de Red	172.XY.3.0 donde XY son los últimos dos dígitos de su cédula.	172.19.3.0
Requerimiento de host Subred LAN1	60	172.19.3.0-63 255.255.255.192/26
Requerimiento de host Subred LAN2	20	172.19.3.64-95 255.255.255.224/27
R1 G0/0/1	Última dirección de host de la subred LAN1	172.19.3.62

R1 G0/0/0	Última dirección de host de la subred LAN2	172.19.3.94
S1 SVI	Segunda dirección de host de la subred LAN1	172.19.3.2
PC-A	Décima dirección de host de la subred LAN1	172.19.3.10
PC-B	Décima dirección de host de la subred LAN2	172.19.3.75

Fuente: UNAD

De acuerdo con los requerimientos, se toma una subred con máscara 26 ya que permite 62 IP utilizables y la segunda con máscara 27 que permite 30 IP utilizables.

Luego, para las interfaces del Router se toman las últimas IP utilizables de cada LAN, esta se asigna teniendo en cuenta el rango, por ejemplo, 172.19.3.63 es el broadcast para LAN1, la última IP utilizable resulta ser 172.19.3.62.

Para el Switch y los PC aplica la misma regla, el conteo parte desde la primera IP utilizable, en LAN1 es 172.19.3.1 y 172.19.3.65 para LAN2.

Por último, las puertas de enlace para cada LAN son las IPs que se configuraron en las interfaces de red del Router.

1.3. Configurar aspectos básicos

1.3.1. Configurar equipos de red

Previo a las tareas solicitadas de la actividad, se debe ingresar a la configuración de la terminal del router con los siguientes comandos:

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Tabla 2 Tareas de configuración en R1

Tarea	Comando
Desactivar la búsqueda DNS	**Router(config)#no ip domain-lookup** // Esto evita que el Router realice búsquedas de DNS cuando se ingrese incorrectamente un comando ya que esa búsqueda bloquea el teclado y genera lentitud.
Nombre del router: *R1*	**Router(config)#hostname R1** // Asignar nombres al Router permite al administrador identificar y gestionar estos dispositivos
Nombre de dominio	**R1(config)#ip domain name ccna-sa.com** // Esto permite que el Router pueda hacer búsquedas de DNS
Contraseña cifrada para el modo EXEC privilegiado	**R1(config)# enable secret ciscoenpass** // Se habilita la contraseña de modo cifrado para ingresar a la configuración de la terminal.
Contraseña de acceso a la consola: *ciscoconpass*	**R1(config)#line console 0** **R1(config-line)#password ciscoconpass** **R1(config-line)#login** // Contraseña de acceso a la consola, se usa el comando login para habilitarla.
Establecer la longitud mínima para las contraseñas: *10*	**R1(config)#security passwords min-length 10** // Refuerza la seguridad evitando que se definan contraseñas con menos de 10 caracteres.
Crear un usuario administrativo en la base de datos local	**R1(config)#username admin password admin1pass** // Permite crear un usuario local para autenticación en el inicio de sesión de la consola.

Configure el inicio de sesión en las líneas VTY para que use la BD local	**R1(config-line)#line vty 0 4** **R1(config-line)#login local** **R1(config-line)#no password** // Controla el acceso por conexiones remotas
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**R1(config-line)#transport input ssh** // Permite que solo se use el canal SSH ya que el más seguro
Cifrar las contraseñas de texto no cifrado	**R1(config-line)#exit** **R1(config)#service password-encryption** // Permite que las contraseñas se cifren y no se vean como son en el archivo de configuración.
Configurar un banner MOTD: *Dispositivo, estudiante y programa.*	**R1(config)#banner motd #R1_RosaLopez_IngenieriaSistemas#** // Permite establecer notificaciones antes del acceso a consola
Configuración de interface G0/0/0: *Descripción, IPv4 y activar la interfaz*.	**R1(config)#interface G0/0/0** **R1(config-if)#description Ruta a LAN2** **R1(config-if)#ip address 172.19.3.94 255.255.255.224** **R1(config-if)#no shutdown** // Se habilita interface para que permita comunicación con LAN2, se define con IP y máscara de subred.
Configuración de interface G0/0/1: *Descripción,*	**R1(config)#interface G0/0/1** **R1(config-if)#description Ruta a S1** **R1(config-if)#ip address 172.19.3.62 255.255.255.192** **R1(config-if)#no shutdown**

IPv4 y activar la interfaz.	// Se habilita interface para que permita comunicación con LAN1, se define con IP y máscara de subred.
Generar una clave de cifrado RSA: *Módulo de 1024 bits*	**R1(config)#crypto key generate rsa** The name for the keys will be: R1.ccna-sa.com How many bits in the modulus [512]: **1024** % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] // Esto permite cifrar los datos en la conexión por SSH, se generan par de llaves de 1024 bits.

Fuente: Autor

Tabla 3 Tareas de configuración de S1

Tarea	Comando
Desactivar la búsqueda DNS	**Switch(config)#no ip domain-lookup** Evita que el Switch realice búsquedas de DNS cuando se ingrese incorrectamente un comando ya que esa búsqueda bloquea el teclado y genera lentitud.
Nombre del switch: *S1*	**Switch(config)#hostname S1** // Asignar un nombre al Switch permite al administrador identificar y gestionar estos dispositivos
Nombre de dominio: *ccna-sa.com*	**S1(config)#ip domain name ccna-sa.com** // Esto permite que el Switch pueda hacer búsquedas de DNS
Contraseña cifrada para el modo EXEC privilegiado	**S1(config)#enable secret ciscoenpass** // Se habilita la contraseña de modo cifrado para ingresar a la configuración de la terminal.
Contraseña de acceso a la	**S1(config)#line console 0** **S1(config-line)#password ciscoconpass** **S1(config-line)#login**

consola: *ciscoconpass*	// Contraseña de acceso a la consola, se usa el comando login para habilitarla.
Apagar todos los puertos sin usar: *F0/1-4, F0/7-24, G0/1-2*	**S1(config)#inter range F0/1-4, F0/7-24, G0/2** **S1(config-if-range)#shutdown** // Por seguridad, se apagan los puertos que no estén en uso con el comando shutdown
Crear un usuario administrativo en la BD local	**S1(config)#username admin password admin1pass** // Permite crear un usuario local para autenticación en el inicio de sesión de la consola.
Configure el inicio de sesión en las líneas VTY para que use la BD local	**S1(config)#line vty 0 4** **S1(config-line)#login local** **S1(config-line)#no password** // Controla el acceso por conexiones remotas con una contraseña
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**S1(config-line)#transport input ssh** // Permite que solo se use el canal SSH para las conexiones remotas
Cifrar las contraseñas de texto no cifrado	**S1(config)#service password-encryption** // Permite que las contraseñas se cifren y no se vean como son en el archivo de configuración.
Configurar un banner MOTD: *Dispositivo, estudiante y programa.*	**S1(config)#banner motd #S1_RosaLopez_IngenieriaSistemas#** // Permite establecer notificaciones antes del acceso a consola
Generar una clave de cifrado	**S1(config)#crypto key generate rsa** **How many bits in the modulus [512]: 1024**

RSA: *Módulo de 1024 bits*	// Esto permite cifrar los datos en la conexión por SSH, se generan par de llaves de 1024 bits.
Configure la interfaz de administración (SVI) en VLAN1: *descripción y dirección IPv4*	**S1(config-if)#description SVI** **S1(config-if)#ip address 172.19.3.2 255.255.255.192** **S1(config-if)#ip default-gateway 172.19.3.62** **S1(config-if)#no shutdown** // Se habilita interface para que permita comunicación por SVI, se define con IP, máscara de subred y puerta de enlace.

Fuente: Autor

1.4. Configurar equipos PC

Tabla 4 Configuración de red de PC-A

Descripción	PC-A
Dirección física	000D.BD62.3963
Dirección IPv4	172.19.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.19.3.62

Fuente: Autor

Tabla 5 Configuración de red de PC-B

Descripción	PC-B
Dirección física	0001.97C3.C3A5
Dirección IPv4	172.19.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.19.3.94

Fuente: Autor

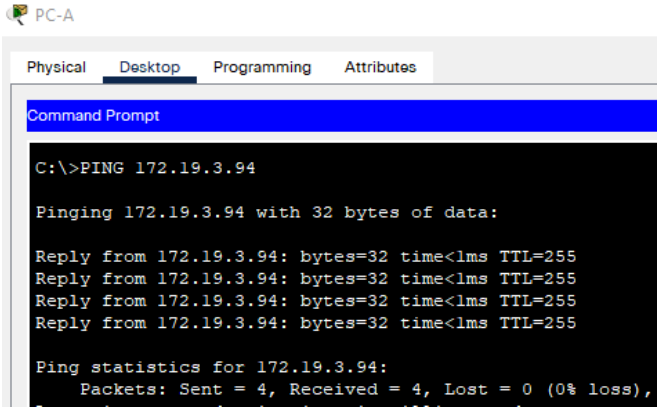
Para diligenciar los datos de la tabla 4 y 5 se tomaron en cuenta los siguientes aspectos:

- La dirección física se obtiene al ingresar a Command Prompt del PC y ejecutar el comando ipconfig /all
- La dirección IPv4, máscara de subred y puerta de enlace se configuran desde Escritorio > Configuración IP del equipo. Estas IP se definieron en la tabla 1.
- La puerta de enlace es la IP que se configuro en la interface del Router que se conecta a la LAN donde se encuentre el PC.

1.5. Probar y verificar la conectividad de extremo a extremo

En la siguiente tabla se verifica la conectividad con cada dispositivo de red:

Tabla 6 Pruebas de conectividad desde PC-A 172.19.3.10

Destino	Descripción	Resultados
R1 G0/0/0 172.19.3.94	Prueba satisfactoria, con todos los paquetes recibidos. Por defecto, el ping envía 4 paquetes, si se requieren más, se debe agregar -t al final del comando.	*Figura 2 Ping de PC-A hacia LAN2*  *Fuente: Autor*

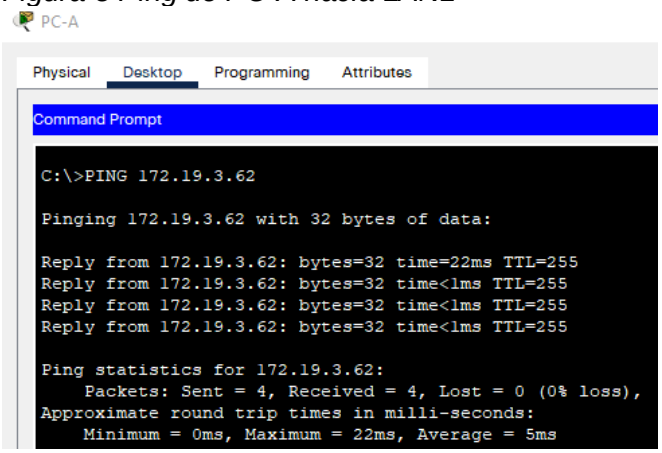
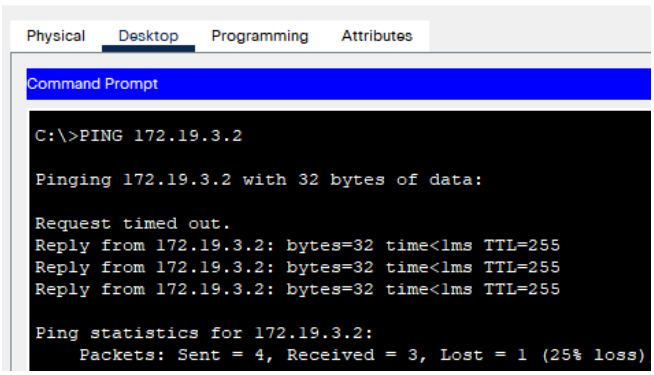
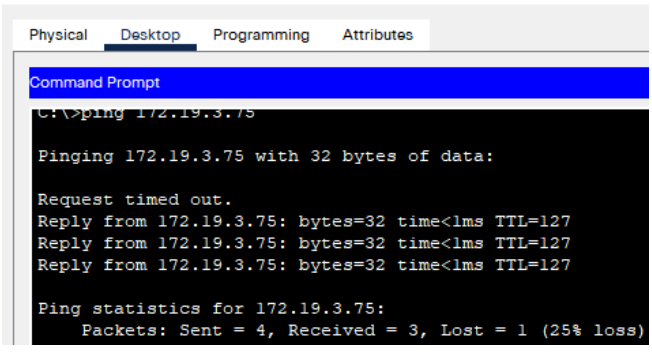
R1 G0/0/1 172.19.3.62	Prueba satisfactoria, con todos los paquetes recibidos.	*Figura 3 Ping de PC-A hacia LAN1*  *Fuente: Autor*
S1 VLAN 1 172.19.3.2	Prueba satisfactoria, con la mayoría de los paquetes recibidos. El primer paquete es posible que se pierda en las primeras pruebas de conectividad.	*Figura 4 Ping de PC-A hacia VLAN1*  *Fuente: Autor*
PC-B 172.19.3.75	Prueba satisfactoria, con la mayoría de los paquetes recibidos. El primer paquete es posible que se pierda en las primeras pruebas de conectividad.	*Figura 5 Ping de PC-A hacia PC-B*  *Fuente: Autor*

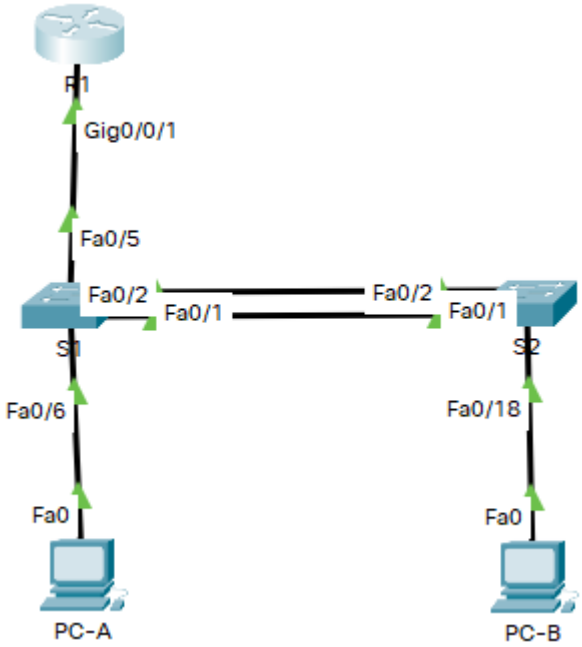
Tabla 7 Pruebas de conectividad desde PC-B 172.19.3.75

Destino	Descripción	Resultados
R1 G0/0/0 172.19.3.94	Prueba satisfactoria, con todos los paquetes recibidos.	*Figura 6 Ping de PC-B hacia LAN2* PC-B Physical Desktop Programming Attributes Command Prompt C:\>ping 172.19.3.94 Pinging 172.19.3.94 with 32 bytes of data: Reply from 172.19.3.94: bytes=32 time<1ms TTL=255 Reply from 172.19.3.94: bytes=32 time<1ms TTL=255 Reply from 172.19.3.94: bytes=32 time<1ms TTL=255 Reply from 172.19.3.94: bytes=32 time<1ms TTL=255 Ping statistics for 172.19.3.94: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) *Fuente: Autor*
R1 G0/0/1 172.19.3.62	Prueba satisfactoria, con todos los paquetes recibidos.	*Figura 7 Ping de PC-B hacia LAN1* PC-B Physical Desktop Programming Attributes Command Prompt C:\>ping 172.19.3.62 Pinging 172.19.3.62 with 32 bytes of data: Reply from 172.19.3.62: bytes=32 time<1ms TTL=255 Reply from 172.19.3.62: bytes=32 time<1ms TTL=255 Reply from 172.19.3.62: bytes=32 time<1ms TTL=255 Reply from 172.19.3.62: bytes=32 time<1ms TTL=255 Ping statistics for 172.19.3.62: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) *Fuente: Autor*
S1 VLAN1 172.19.3.2	Prueba satisfactoria, con todos los paquetes recibidos.	*Figura 8 Ping de PC-B hacia SVI* PC-B Physical Desktop Programming Attributes Command Prompt Pinging 172.19.3.2 with 32 bytes of data: Reply from 172.19.3.2: bytes=32 time<1ms TTL=254 Reply from 172.19.3.2: bytes=32 time=15ms TTL=254 Reply from 172.19.3.2: bytes=32 time<1ms TTL=254 Reply from 172.19.3.2: bytes=32 time<1ms TTL=254 Ping statistics for 172.19.3.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) *Fuente: Autor*

Fuente: Autor

2. ESCENARIO 2

Figura 9 Topología para el escenario 2



Fuente: Autor

Para el desarrollo de este escenario se utilizaron:

- 1 Router 4331
- 2 switch 2960
- 2 PC

Tabla 8 VLAN para Escenario 2

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

Fuente: UNAD

Tabla 9 Asignación de direcciones para el Escenario 2

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.19.8.1/26 2001:db8:acad:a::1/64	No corresponde
R1 G0/0/1.30	10.19.8.65/27 2001:db8:acad:b::1/64	No corresponde
R1 G0/0/1.40	10.19.8.97/29 2001:db8:acad:c::1/64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1/27 2001:db8:acad:209::1/64	No corresponde
S1 VLAN 4	10.19.8.98/29 2001:db8:acad:c::99/64 fe80::99	10.19.8.97 No corresponde No corresponde
S2 VLAN 4	10.19.8.99/29 2001:db8:acad:c::99/64 fe80::99	10.19.8.97 No corresponde No corresponde
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a::50/64	DHCP para default gateway IPv4 fe80::1
PC-B NIC	Dirección DHCP para IPv4 2001:db8:acad:b::50/64	DHCP para default gateway IPv4 fe80::1

Fuente: UNAD

2.1. Inicializar, recargar y configurar aspectos básicos de los dispositivos

2.1.1. Inicializar y volver a cargar el router y el switch

- Borrar las configuraciones de inicio y las VLAN del router y del switch y volver a cargar los dispositivos.

  Router

R1>enable
R1#delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (No such file or directory)
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
R1#reload
System configuration has been modified. Save? [yes/no]:y
Building configuration...
[OK]
Proceed with reload? [confirm]
Initializing Hardware ...

Switch 1 y 2

Switch>
Switch>enable
Switch#delete vlan.data
Switch#erase startup-config
Switch#reload

El comando delete vlan.data elimina la información que se tuviera de VLAN y luego con el comando erase startup-config se borra la configuración de inicio y luego se reinicia el dispositivo.

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

Switch 1

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

Para este punto se ejecutan los mismos comandos en el Switch 2. Con el comando sdm prefer dual-ipv4-and-ipv6 default activa una plantilla del Switch Database Management (SDM) que otorga más recursos al enrutamiento IPv4 e IPv6. Por último, se reinicia el Switch para que tome los cambios.

2.1.2. Configurar R1

Tabla 10 Ajustes en R1

Tarea	Comando
Desactivar la búsqueda DNS	**Router(config)#no ip domain-lookup** // Esto evita que el Router realice búsquedas de DNS cuando se ingrese incorrectamente un comando ya que esa búsqueda bloquea el teclado y genera lentitud.
Nombre del router: *R1*	**Router(config)#hostname R1** // Asignar nombres al Router permite al administrador identificar y gestionar estos dispositivos
Nombre de dominio: *ccna-sa.com*	**R1(config)#ip domain name ccna-sa.com** // Esto permite que el Router pueda hacer búsquedas de DNS

Contraseña cifrada para el modo EXEC privilegiado: *class*	**R1(config)# enable secret class** // Se habilita la contraseña de modo cifrado para ingresar a la configuración de la terminal.
Contraseña de acceso a la consola: *cisco*	**R1(config)#line console 0** // Ingreso ajustes de consola **R1(config-line)#password cisco** //Se define contraseña **R1(config-line)#login** // Habilita la contraseña
Establecer la longitud mínima para contraseñas	**R1(config)#security passwords min-length 5** // Refuerza la seguridad evitando que se definan contraseñas con menos de 5 caracteres.
Crear un usuario administrativo en la base de datos local	**R1(config)#username admin password admin1pass** // Permite crear un usuario local para autenticación en el inicio de sesión de la consola.
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	**R1(config-line)#line vty 0 4** // Ingresar a los ajustes de conexiones remotas **R1(config-line)#login local** //Habilita el inicio de sesión solo para la cuenta local creada
Configurar VTY solo aceptando SSH	**R1(config-line)#transport input ssh** // Permite que solo se use el canal SSH ya que el más seguro
Cifrar las contraseñas de texto no cifrado	**R1(config)#service password-encryption** // Permite que las contraseñas se cifren y no se vean como son en el archivo de configuración.
Configurar un banner MOTD: *Dispositivo, estudiante y programa.*	**R1(config)#banner motd #R1_RosaLopez_IngenieriaSistemas#** // Permite establecer notificaciones al iniciar el acceso a la consola

Habilitar el routing IPv6	**R1(config)#ipv6 unicast-routing** // Permite configurar cualquier protocolo de routing IPv6.
Configurar interfaz G0/0/1 y subinterfaces: *Establecer descripción, dirección IPv4, dirección local de enlace IPv6 como fe80: :1, dirección IPv6 y activar la interfaz*.	**R1(config)#inter g0/0/1** // Ingresar a la interfaz **R1(config-if)#int g0/0/1.20** // Ingresar a la subinterfaz **R1(config-subif)#description interface vlan20** //Agregar descripción a la subinterfaz **R1(config-subif)#encapsulation dot1Q 20** // Se asigna VLAN 20 a esta subinterfaz **R1(config-subif)#ip add 10.19.8.1 255.255.255.192** // Se asigna IPv4 y máscara a esta subinterfaz. **R1(config-subif)#ipv6 add fe80::1 link-local** //Se asigna IPv6 link local. **R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64** // Se asigna IPv6 y máscara a esta subinterfaz. **R1(config-subif)#no shut** // Se habilita interfaz --- **R1(config-subif)#int g0/0/1.30** **R1(config-subif)#description interface vlan30** **R1(config-subif)#encapsulation dot1Q 30** **R1(config-subif)#ip add 10.19.8.65 255.255.255.224** **R1(config-subif)#ipv6 add fe80::1 link-local** **R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64** **R1(config-subif)#no shut** --- **R1(config-if)#int g0/0/1.40** **R1(config-subif)#description interface vlan40** **R1(config-subif)#encapsulation dot1Q 40** **R1(config-subif)#ip add 10.19.8.97 255.255.255.248** **R1(config-subif)#ipv6 add fe80::1 link-local**

	R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 **R1(config-subif)#no shut** --- **R1(config-subif)#int g0/0/1.56** **R1(config-subif)#encapsulation dot1Q 56** **R1(config-subif)#no shut**
Configurar Loopback0 interface	**R1(config)#inter loopback 0** **R1(config-if)#ip add 209.165.201.1 255.255.255.224** **R1(config-if)#ipv6 add 2001:db8:acad:209::1/64** **R1(config-if)#ipv6 add fe80::1 link-local** **R1(config-if)#no shut** // La interfaz loopback es una interfaz lógica del router. Permite probar y administrar el Router como una interfaz disponible.
Generar una clave de cifrado RSA: *Módulo de 1024 bits*	**R1(config)#crypto key generate rsa** The name for the keys will be: R1.ccna-sa.com How many bits in the modulus [512]: **1024** % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] // Esto permite cifrar los datos en la conexión por SSH, se generan par de llaves de 1024 bits.

Fuente: Autor

Al terminar los ajustes, se ejecuta el comando show running-config y show ip inter brief para determinan que estén correctos.

R1#show running-config
Building configuration...
Current configuration : 2185 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 5

```
!
hostname R1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip cef
ipv6 unicast-routing
!
username admin password 7 082048430017540713181F
!
no ip domain-lookup
ip domain-name ccna-sa.com
!
spanning-tree mode pvst
!
interface Loopback0
 ip address 209.165.201.1 255.255.255.224
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:209::1/64
!
interface GigabitEthernet0/0/1
 description Ruta a S1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
!
interface GigabitEthernet0/0/1.20
 description interface vlan20
 encapsulation dot1Q 20
 ip address 10.19.8.1 255.255.255.192
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/0/1.30
 description interface vlan30
 encapsulation dot1Q 30
 ip address 10.19.8.65 255.255.255.224
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:B::1/64
!
interface GigabitEthernet0/0/1.40
 description interface vlan40
 encapsulation dot1Q 40
 ip address 10.19.8.97 255.255.255.248
```

ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:C::1/64

Figura 10 Ver características de las interfaces de R1

```
R1#show ip inter brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES manual administratively down down
GigabitEthernet0/0/1   unassigned      YES manual up                    up
GigabitEthernet0/0/1.2010.19.8.1       YES manual up                    up
GigabitEthernet0/0/1.3010.19.8.65      YES manual up                    up
GigabitEthernet0/0/1.4010.19.8.97      YES manual up                    up
GigabitEthernet0/0/1.56unassigned      YES unset  up                    up
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
Loopback0              209.165.201.1   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Fuente: autor

En la figura 10 se evidencia que las interfaces que no se utilizan están apagadas y las que están funcionando tienen su respectiva configuración de IP.

2.1.3. Configurar S1 y S2

Tabla 11 Configurar S1 y S2

Tarea	Comando
Desactivar la búsqueda DNS	**Switch(config)#no ip domain-lookup** // Evita que el Switch realice búsquedas de DNS cuando se ingrese incorrectamente un comando ya que esa búsqueda bloquea el teclado y genera lentitud.
Nombre del switch: *S1*	**Switch(config)#hostname S1** **Switch(config)#hostname S2** // Asignar un nombre al Switch permite al administrador identificar y gestionar estos dispositivos
Nombre de dominio: *ccna-sa.com*	**S1(config)#ip domain name ccna-sa.com** // Esto permite que el Switch pueda hacer búsquedas de DNS

Contraseña cifrada para el modo EXEC privilegiado	**S1(config)#enable secret class** // Se habilita la contraseña de modo cifrado para ingresar a la configuración de la terminal.
Contraseña de acceso a la consola: *cisco*	**S1(config)#line console 0** **S1(config-line)#password cisco** **S1(config-line)#login** // Contraseña de acceso a la consola, se usa el comando login para habilitarla.
Crear un usuario administrativo en la BD local	**S1(config)#username admin password admin1pass** // Permite crear un usuario local para autenticación en el inicio de sesión de la consola.
Configure el inicio de sesión en las líneas VTY para que use la BD local	**S1(config)#line vty 0 4** **S1(config-line)#login local** // Controla el acceso por conexiones remotas con una contraseña
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**S1(config-line)#transport input ssh** // Permite que solo se use el canal SSH para las conexiones remotas
Cifrar las contraseñas de texto no cifrado	**S1(config)#service password-encryption** // Permite que las contraseñas se cifren y no se vean como son en el archivo de configuración.
Configurar un banner MOTD: *Dispositivo, estudiante y programa.*	**S1(config)#banner motd #S1_RosaLopez_IngenieriaSistemas#** // Permite establecer notificaciones antes del acceso a consola

Generar una clave de cifrado RSA: *Módulo de 1024 bits*	**S1(config)#crypto key generate rsa** How many bits in the modulus [512]: **1024** // Esto permite cifrar los datos en la conexión por SSH, se generan par de llaves de 1024 bits.
Configure la interfaz de administración (SVI) en VLAN 40: *dirección IPv4, dirección local, dirección IPv6 y gateway*	**S1(config)#inter vlan 40** **S1(config-if)#ip add 10.19.8.98 255.255.255.248** **S1(config-if)#ipv6 add fe80::98 link-local** **S1(config-if)#ipv6 add 2001:db8:acad:c::98/64** **S1(config-if)#ip default-gateway 10.19.8.97** --- **S2(config)#inter vlan 40** **S2(config-if)#ip add 10.19.8.99 255.255.255.248** **S2(config-if)#ipv6 add fe80::99 link-local** **S2(config-if)#ipv6 add 2001:db8:acad:c::99/64** **S2(config-if)#ip default-gateway 10.19.8.97** // Se habilita interface para que permita comunicación por SVI, se define con IPv4 e IPv6, máscara de subred y puerta de enlace IPv4.

Fuente: Autor

2.2. Configurar infraestructura de red (VLAN, Trunking, EtherChannel)

2.2.1. Configurar S1

Tabla 12 Configurar infraestructura de red en S1

Tarea	Comando
Crear VLAN de acuerdo con la tabla 8	**S1(config)#vlan 20** **S1(config-vlan)#name Docentes** **S1(config)#vlan 30** **S1(config-vlan)#name Estudiantes**

	S1(config-vlan)#vlan 40 **S1(config-vlan)#name Invitados** **S1(config-vlan)#vlan 50** **S1(config-vlan)#name Usuarios** **S1(config-vlan)#vlan 56** **S1(config-vlan)#name Native** **S1#show vlan** // Verificar que las VLAN estén correctas
Crear puerto troncal 802.1Q que utilicen la VLAN 56 como nativa	**S1(config-if)#inter range f0/1-2, f0/5** **S1(config-if-range)#switchport mode trunk** **S1(config-if-range)#switchport trunk native vlan 56** **S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56** **S1#show inter f0/2 switchport** // La VLAN nativa se cambia a VLAN 56 y la lista de VLAN permitidas se restringe a 20,30,40,50 y 56. 802.1Q es un método de encapsulación para enlaces troncales.
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1, F0/2 y F0/5. Usar el protocolo LACP para la negociación	**S1(config)#int range f0/1-2** **S1(config-if-range)#channel-group 1 mode active** **S1(config)#inter port-channel 1** **S1(config-if-range)#switchport mode trunk** **S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56** **S1#show etherchannel summary** // Un EtherChannel es cuando se ajustan interfaces en dos switches para versen en paralelo. Con LCAP se especifican las interfaces, se crea la interfaz port-channel y se cambia la configuración de capa 2.
Configurar el puerto de acceso	**S1(config)#inter f0/6** **S1(config-if)#switchport mode access**

de host para VLAN 20 en la Interface F0/6	**S1(config-if)#switchport access vlan 20** // Se ingresa a la interfaz y se configura modo acceso con la vlan 20
Configurar la seguridad del puerto en los puertos de acceso. Permitir 4 direcciones MAC	**S1(config)#inter f0/6** **S1(config-if)#switchport port-security** **S1(config-if)#switchport port-security maximum 4** **S1(config-if)#switchport port-security violation shutdown** **S1(config-if)#switchpor port-security mac-address sticky** // Se ingresa a la interfaz y se define el máximo de direcciones MAC permitidas.
Configurar puerto troncal en G0/1	
Proteja todas las interfaces no utilizadas. Asignar a VLAN 50, Establecer en modo de acceso y apagar	**S1(config)#inter 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)#shut** **S1(config-if-range)#switchport port-security** **S1(config-if-range)#switchport port-security violation shutdown** // Se ingresan a las interfaces por rango ya que los ajustes son los mismos, se configura modo acceso con la vlan 50 y se apagan las interfaces.

Fuente: Autor

Tabla 13 Configurar infraestructura de red en S2

Tarea	Comando
Crear VLAN	**S2(config)#vlan 20** **S2(config-vlan)#name Docentes** **S2(config-vlan)#vlan 30**

	S2(config-vlan)#name Estudiantes **S2(config-vlan)#vlan 40** **S2(config-vlan)#name Invitados** **S2(config-vlan)#vlan 50** **S2(config-vlan)#name Usuarios** **S2(config-vlan)#vlan 56** **S2(config-vlan)#name Native** **S1#show vlan** // Verificar que las VLAN estén correctas
Crear puertos troncales 802.1Q que utilicen la VLAN 56 como nativa	**S2(config)#inter range f0/1-2** **S2(config-if-range)#switchport mode trunk** **S2(config-if-range)#switchport trunk native vlan 56** **S2#show inter f0/2 switchport** // Interfaces F0/1 y F0/2 se toman como un rango y se configuran en modo troncal con la vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Usar el protocolo LACP para la negociación	**S2(config)#inter range f0/1-2** **S2(config-if-range)#channel-group 1 mode active** **S2(config)#inter port-channel 1** **S2(config-if-range)#switchport mode trunk** **S2(config-if)#switchport trunk allowed vlan 20,30,40,50,56** **S1#show etherchannel summary** // Un EtherChannel es cuando se ajustan interfaces en dos switches para versen en paralelo. Con LCAP se especifican las interfaces, se crea la interfaz port-channel y se cambia la configuración de capa 2.
Configurar el puerto de acceso de host para VLAN 30 en la Interface F0/18	**S2(config)#inter f0/18** **S2(config-if)#switchport mode access** **S2(config-if)#switchport access vlan 30** // Se ingresa a la interfaz y se configura modo acceso con la vlan 30 **S2(config-if)#end**

	S2#show vlan brief **S2#show int f0/18 sw** // Se revisa si los ajustes del puerto con la VLAN están correctos.
Configurar la seguridad del puerto en los puertos de acceso. Permitir 4 direcciones MAC	**S2(config)#inter f0/18** **S2(config-if)#switchport port-security** // Habilita la seguridad del puerto **S2(config-if)#switchport port-security maximum 4** // Número máximo de direcciones MAC seguras **S2(config-if)#switchport port-security violation shutdown** //Apagar el puerto si se conecta una Mac no segura **S2(config-if)#switchport port-security mac-address sticky** // Para que aprenda la dirección Mac automáticamente **S2#show port-security inter f0/18** // Ver los ajustes realizados
Proteja todas las interfaces no utilizadas. Asignar a VLAN 50, Establecer en modo de acceso y apagar	**S2(config-if)#inter range g0/1-2, f0/3-17, f0/19-24** **S2(config-if-range)#switchport mode access** **S2(config-if-range)#switchport access vlan 50** **S2(config-if-range)#shut** **S2(config-if-range)#switchport port-security** **S2(config-if-range)#switchport port-security violation shutdown** // Se ingresa a las interfaces por rango ya que los ajustes son los mismos, se configura modo acceso con la VLAN 50, se apagan las interfaces y se habilita seguridad en el puerto.

Fuente: Autor

2.3. Configurar soporte de host

2.3.1. Configurar R1

Tabla 14 Configurar soporte en R1

Tarea	Comando
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 20. Crear grupo: -Definir puerta de enlace predeterminada como dirección de interfaz del router -Nombrar dominio unad-ccna-sa.net -Habilitar últimas 10 direcciones de la subred.	**R1(config)#ip dhcp pool vlan20** // Crear grupo **R1(dhcp-config)#network 10.19.8.0 255.255.255.192** //Definir grupo de direcciones **R1(dhcp-config)#default-router 10.19.8.165** //Establecer interfaz del router como puerta de enlace predeterminada **R1(dhcp-config)#domain-name unad-ccna-sa.net** //Establecer dominio **R1(dhcp-config)#ip dhcp excluded-address 10.19.8.2 10.19.8.52** //Excluir direcciones IP para solo dejar habilitadas las necesarias
Configurar DHCP IPv4 para VLAN 3 Crear grupo: -Definir puerta de enlace predeterminada como dirección de interfaz del router -Nombrar dominio unad-ccna-sb.net	**R1(config)#ip dhcp pool vlan30** // Crear grupo **R1(dhcp-config)#network 10.19.8.64 255.255.255.224** //Definir grupo de direcciones **R1(dhcp-config)#default-router 10.19.8.65** //Establecer interfaz del router como puerta de enlace predeterminada **R1(dhcp-config)#domain-name unad-ccna-sb.net** //Establecer dominio **R1(dhcp-config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84** //Excluir direcciones IP para solo dejar habilitadas las necesarias

-Habilitar últimas 10 direcciones de la subred.	
Verificar ajustes	**R1#show running-config | section dhcp** //Ver los comandos DHCPv4 **R1#show ip dhcp binding** // Ver direcciones MAC que usan el servicio DHCPv4

Fuente: Autor

2.3.2. Configurar los servidores

Tabla 15 Configuración de red de PC-A

Descripción	Se muestran los detalles con el comando ipconfig /all
Dirección física	000D.BD62.3963
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Puerta de enlace predeterminado	10.19.8.1
Puerta de enlace IPv6 predeterminada	FE80::1

Fuente: Autor

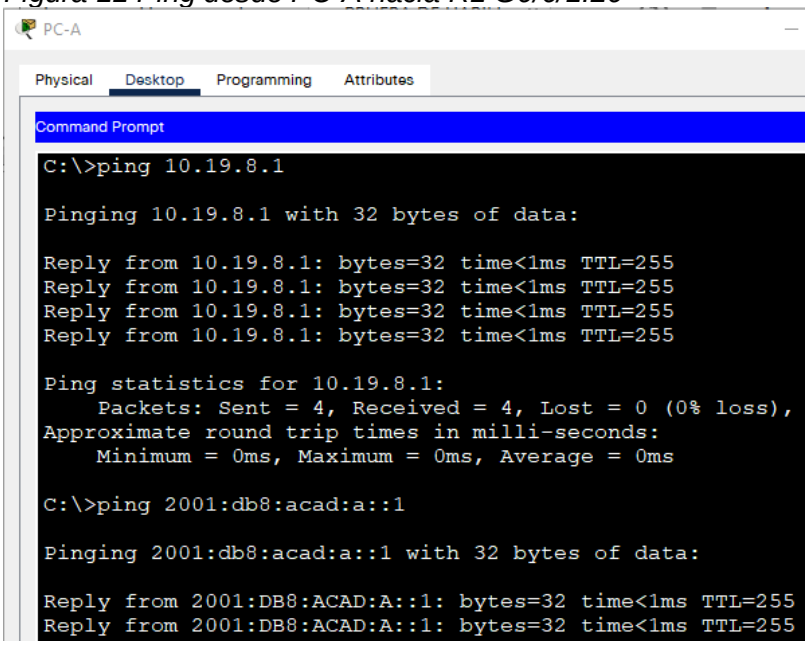
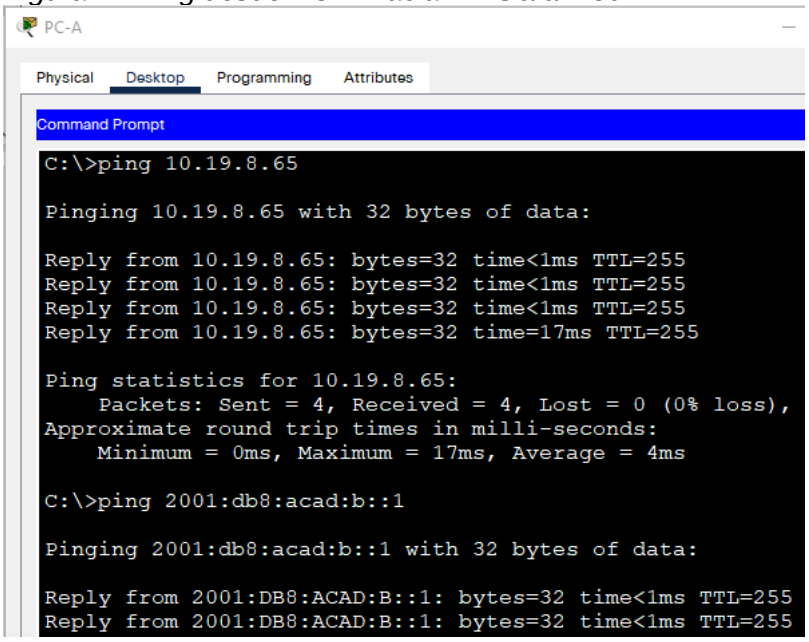
Tabla 16 Configuración de red de PC-B

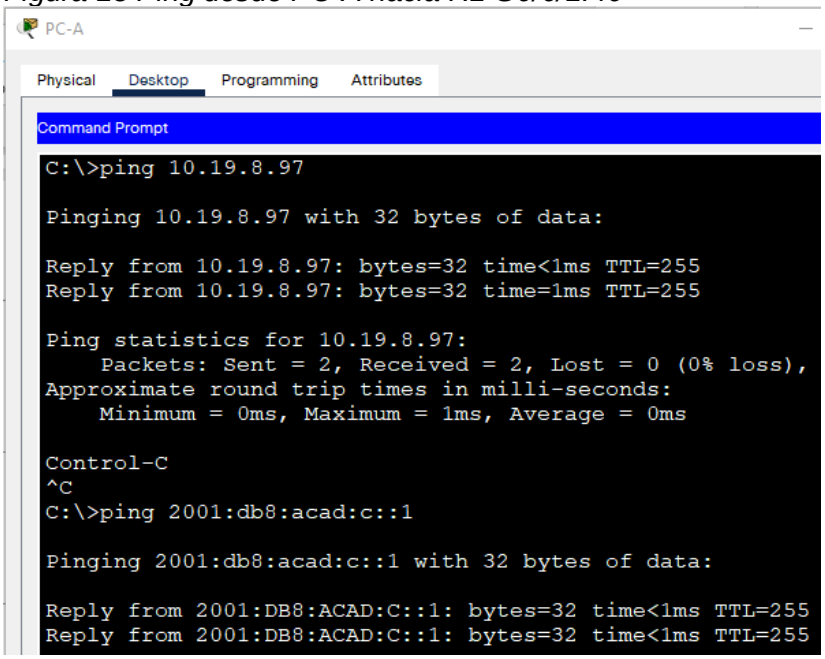
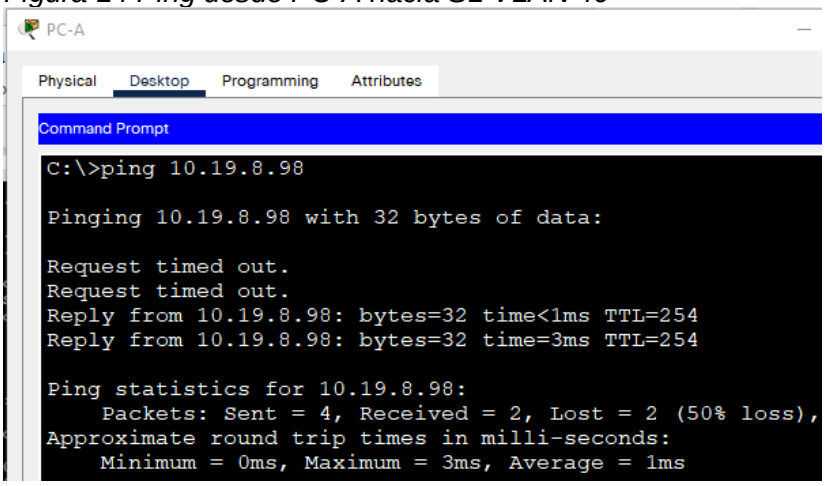
Descripción	Se muestran los detalles con el comando ipconfig /all
Dirección física	0001.97C3.C3A5
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Puerta de enlace predeterminado	10.19.8.65
Puerta de enlace IPv6 predeterminada	FE80::1

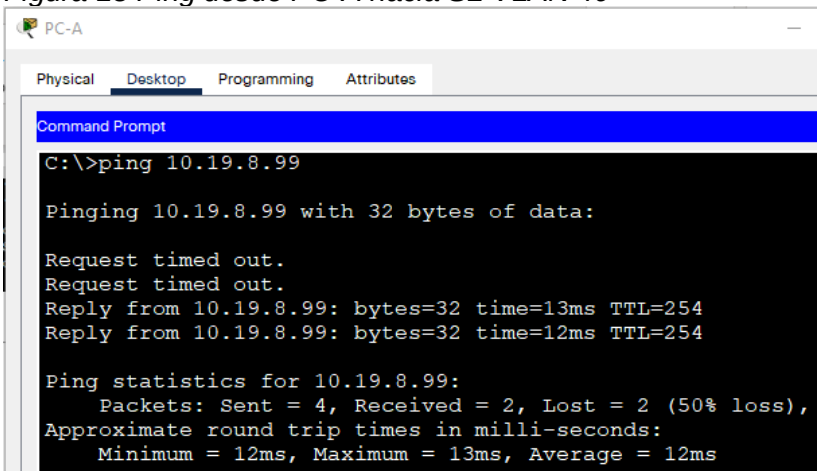
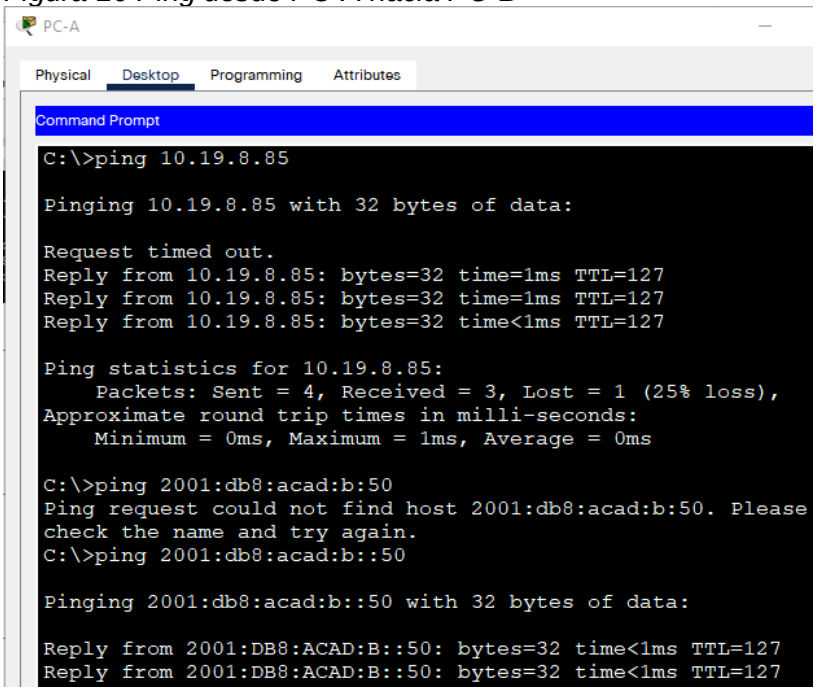
Fuente: Autor

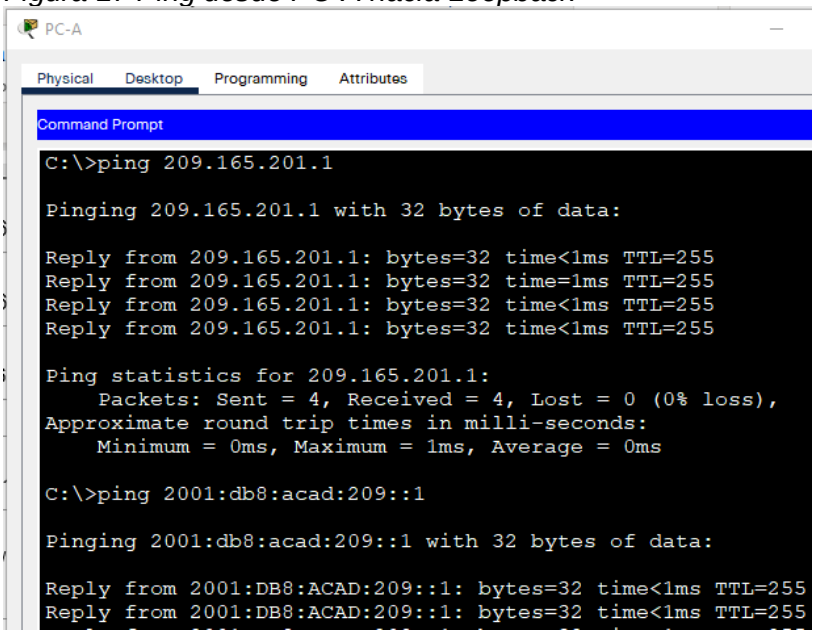
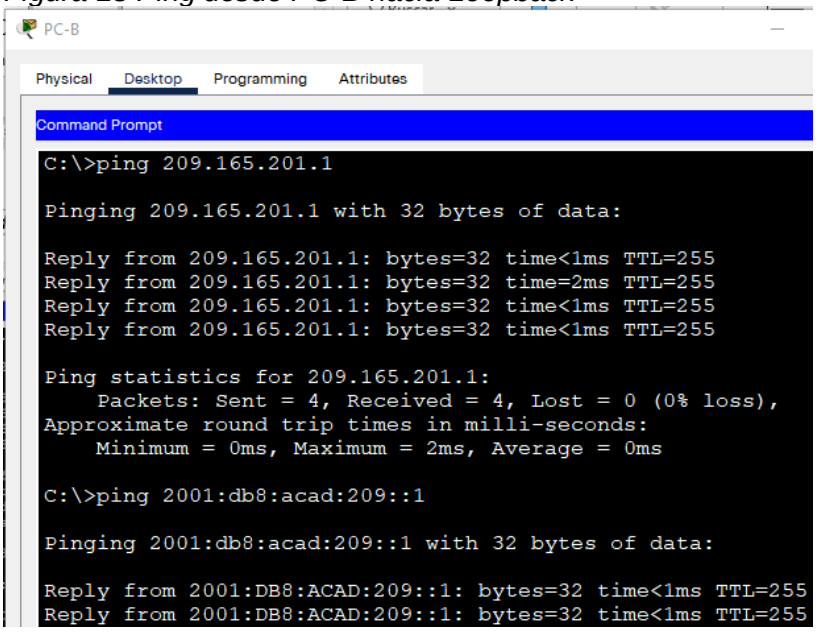
2.4. Probar y verificar la conectividad de extremo a extremo

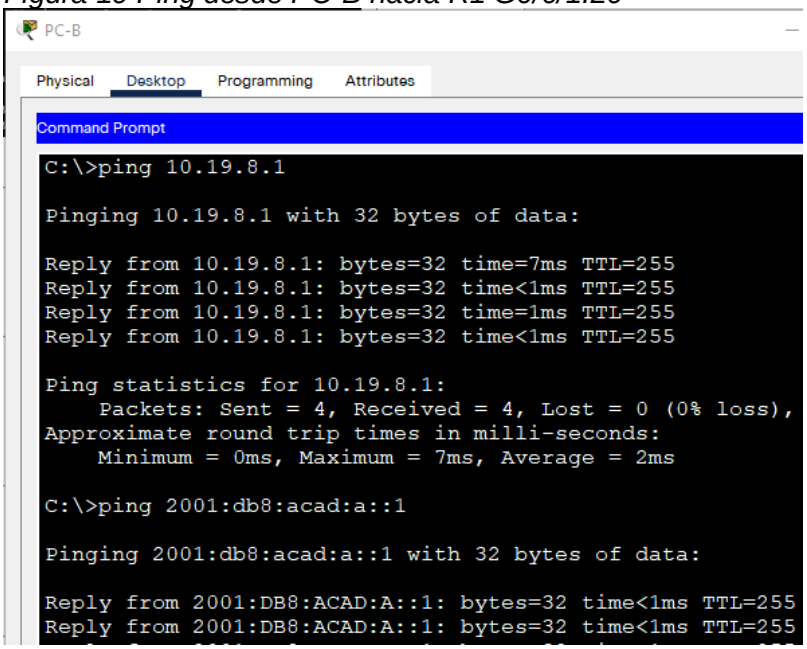
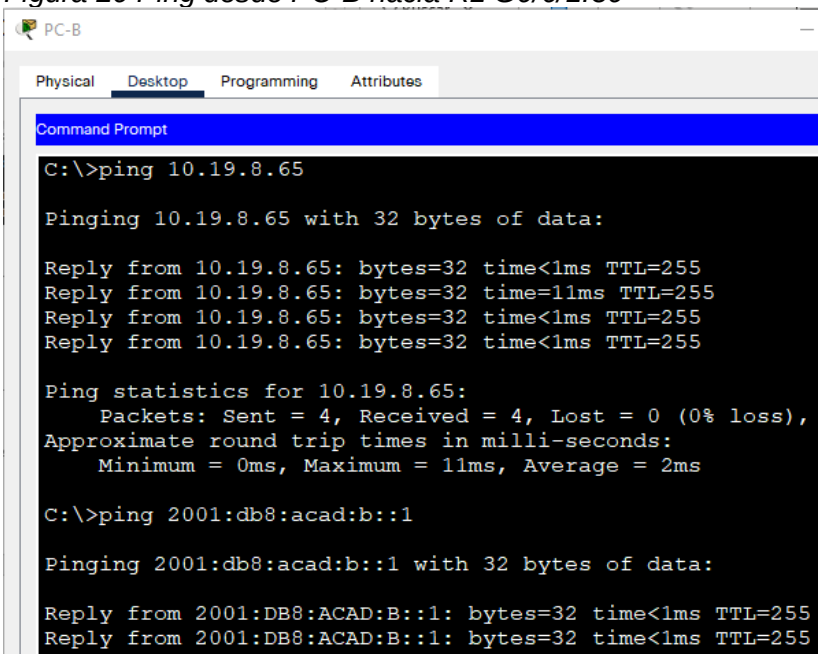
Tabla 17 Verificar conectividad Escenario 2

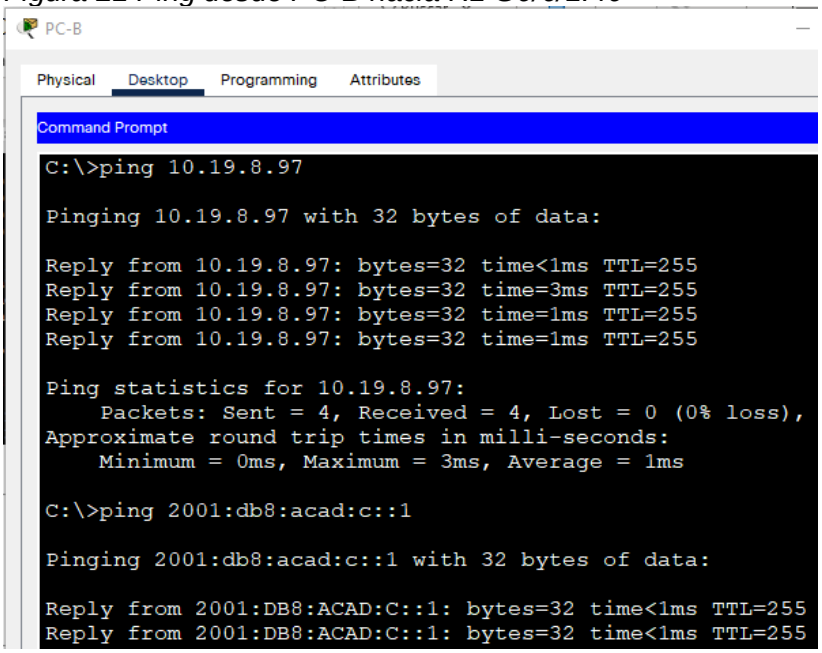
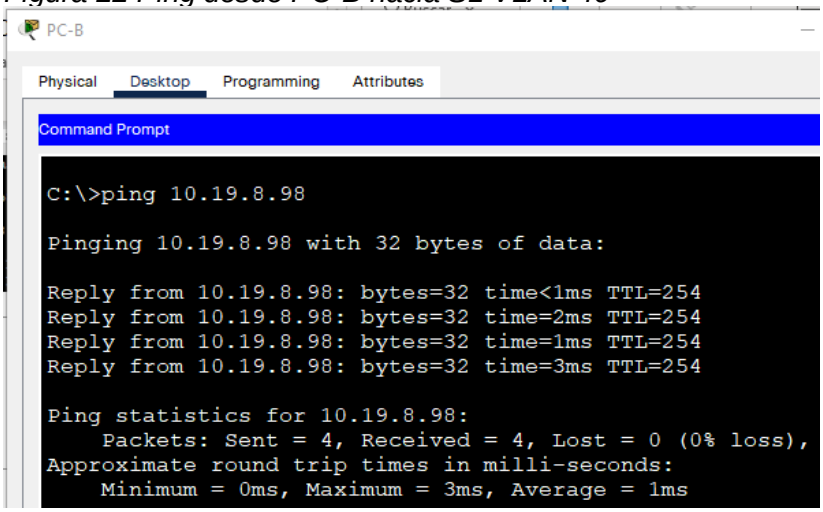
Destino	Resultados
PC-A R1 G0/0/1.20 10.19.8.1 2001:db8:acad:a::1 Resultado: correcto	*Figura 11 Ping desde PC-A hacia R1 G0/0/1.20*  Fuente: Autor
PC-A R1 G0/0/1.30 10.19.8.65 2001:db8:acad:b::1 Resultado: correcto	*Figura 12 Ping desde PC-A hacia R1 G0/0/1.30*  Fuente: Autor

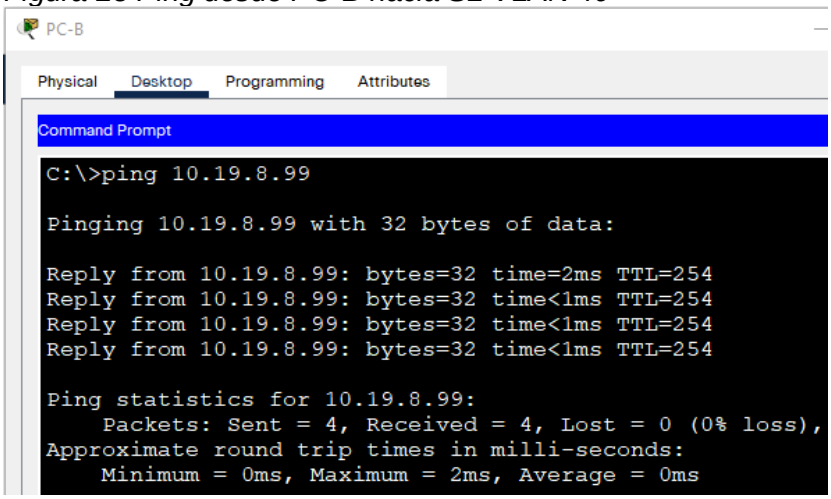
PC-A R1 G0/0/1.40 10.19.8.97 2001:db8:acad:c::1 Resultado: correcto	*Figura 13 Ping desde PC-A hacia R1 G0/0/1.40*  Fuente: Autor
PC-A S1 VLAN 40 10.19.8.98 2001:db8:acad:c::98 Resultado: Correcto en IPv4, IPv6 presenta conflicto causado por error del dispositivo.	*Figura 14 Ping desde PC-A hacia S1 VLAN 40*  Fuente: Autor

PC-A S2 VLAN 40 10.19.8.99 2001:db8:acad:c::99 Resultado: Correcto en IPv4, IPv6 presenta conflicto causado por error del dispositivo.	*Figura 15 Ping desde PC-A hacia S2 VLAN 40*  Fuente: autor
PC-A PC-B 10.19.8.85 2001:db8:acad:b::50 Resultado: correcto	*Figura 16 Ping desde PC-A hacia PC-B*  Fuente: Autor

PC-A R1 Bucle 0 209.165.201.1 2001:db8:acad:209::1 (Loopback) Resultado: correcto	*Figura 17 Ping desde PC-A hacia Loopback*  Fuente: Autor
PC-B R1 Bucle 0 209.165.201.1 2001:db8:acad:209::1 (Loopback) Resultado: correcto	*Figura 18 Ping desde PC-B hacia Loopback*  Fuente: Autor

PC-B G0/0/1.20 10.19.8.1 2001:db8:acad:a::1 Resultado: correcto	*Figura 19 Ping desde PC-B hacia R1 G0/0/1.20*  Fuente: Autor
PC-B R1 G0/0/1.30 10.19.8.65 2001:db8:acad:b::1 Resultado: correcto	*Figura 20 Ping desde PC-B hacia R1 G0/0/1.30*  Fuente: Autor

PC-B R1 G0/0/1.40 10.19.8.97 2001:db8:acad:c::1 Resultado: correcto	*Figura 21 Ping desde PC-B hacia R1 G0/0/1.40*  Fuente: Autor
PC-B S1 VLAN 40 10.19.8.98 2001:db8:acad:c::98 Resultado: Correcto en IPv4, IPv6 presenta conflicto causado por error del dispositivo.	*Figura 22 Ping desde PC-B hacia S1 VLAN 40*  Fuente: Autor

PC-B S2 VLAN 40 10.19.8.99 2001:db8:acad:c::99 Resultado: Correcto en IPv4, IPv6 presenta conflicto causado por error del dispositivo.	*Figura 23 Ping desde PC-B hacia S2 VLAN 40*  Fuente: Autor

Fuente: Autor

CONCLUSIONES

Las actividades realizadas en el primer escenario comprenden los primeros pasos en la configuración de una red donde se incluye la asignación de IPv4 con su respectiva máscara y puerta de enlace; a nivel de seguridad para el acceso a los dispositivos de red y las pruebas de ping en la cual se puede evidenciar si se configuraron las puertas de enlace correctamente para poder alcanzar otras LAN.

Por otro lado, el escenario 2 adiciona más complejidad al establecer comunicación de los dispositivos finales mediante IPv4 e IPv6 y un grupo de puertos EtherChannel entre los dos switches, este escenario brinda mayor acercamiento a redes de empresas grandes donde la redundancia juega un papel importante en la conectividad.

Estos escenarios son los más comunes en las empresas, los dispositivos Cisco permiten simular estas conexiones antes de pasar a un nivel productivo y aunque no todas las empresas manejan dispositivos Cisco, si manejan dispositivos de red donde se debe realizar el mismo proceso aunque si pueden cambiar cosas más específicas como la combinación de comandos para lograr lo requerido.

BIBLIOGRAFÍA

CISCO, Netacad. Introducción a las redes – LAN y WAN (2022) {28 de octubre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/1.4.2

CISCO, Netacad. Introducción a las redes - Estructura básica de comandos de IOS (2022) {30 de octubre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/2.3.1

CISCO, Netacad. Introducción a las redes – Encriptación de las contraseñas (2022) {3 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/2.4.4

CISCO, Netacad. Introducción a las redes – Configuración de interfaz virtual de switch (2022) {3 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/2.7.4

CISCO, Netacad. Introducción a las redes – Protocolos (2022) {4 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/3.2.1

CISCO, Netacad. Introducción a las redes – Dirección MAC de Ethernet (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/7.2.2

CISCO, Netacad. Introducción a las redes – Paquete IPv4 (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/8.2.1

CISCO, Netacad. Introducción a las redes – Paquete IPv6 (2022) {5 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/8.3.1

CISCO, Netacad. Introducción a las redes – Mensajes ICMP (2022) {10 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/itn-dl/13.1.1

CISCO, Netacad. Conmutación, Enrutamiento y redes inalámbricas esenciales – VLANs (2022) {20 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/srwe-dl/3.1.1

CISCO, Netacad. Introducción a las redes – Funcionamiento de EtherChannel (2022) {21 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/srwe-dl/6.1.1

CISCO, Netacad. Introducción a las redes – Protocolos de negociación automática (2022) {21 de noviembre de 2022}. Disponible en https://contenthub.netacad.com/srwe-dl/6.1.5

ANEXOS

Anexo A - Enlace de descarga de archivos de simulación 1

PruebaHabilidades_Escenario1.pkt

Anexo B - Enlace de descarga de archivos de simulación 2

PruebaHabilidades_Escenario2.pkt