

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

FABIAN ANDRES LANCHEROS PINZON

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 TECNOLOGÍA CISCO

FABIAN ANDRES LANCHEROS PINZON

Diplomado de opción de grado presentado para optar
el título de INGENIERIA 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 Jurado

Firma del Jurado

BOGOTA, 22 de noviembre de 2022

AGRADECIMIENTOS

Doy gracias a mi familia por acompañarme en este proceso de formación académica la cual me ha permitido mejorar mi vida poco a poco permitiendo utilizar los conocimientos adquiridos en el ámbito laboral y personal.

También un agradecimiento especial a la universidad a los tutores que a lo largo de esta formación nos han colaborado y a toda su red de colaboradores los cuales nos han brindado una gran ayuda para poder tener una formación optima brindándonos sus conocimientos para el proceso de formación que hemos tenido a lo largo de la carrera.

TABLA DE CONTENIDO

TABLA DE CONTENIDO.....	5
LISTA DE TABLAS	8
LISTA DE FIGURAS	9
GLOSARIO	10
RESUMEN	12
ABSTRACT	13
INTRODUCCIÓN	14
ESCENARIO 1	15
1.1 Escenario 1	15
1.2 CALCULO DIRECCIONAMIENTO IP.....	16
1.3 CONFIGURACION ROUTER R1	17
1.3.1 ROUTER R1	17
1.4 CONFIGURACION S1	20
1.5 CONFIGURACION DE LOS EQUIPOS.....	23
1.5.1 EQUIPO A.....	23
1.5.2 EQUIPO B.....	24
1.6 PROBAR Y VERIFICAR CONECTIVIDAD.....	25
1.6.2 DE PC-A A R1 G0/0/1.....	27
2. ESCENARIO 2	30
2.1 Escenario 2	30
2.2 Simulación del escenario 2	30
2.3 CONFIGURACION.....	31
2.3.1 Asignación de direcciones.....	31

2.4 INSTRUCCIONES ESCENARIO 2.....	33
2.4.1 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos.....	33
2.4.1.1 Paso 1: Inicializar y volver a cargar el router y el switch	33
TAREA	33
ESPECIFICACION.....	33
Ingresar al modo privilegiado	33
Router>enable.....	33
Restaurar valores predeterminados	33
Router#erase startup-config.....	33
Reiniciar el Router.....	33
Router#reload	33
TAREA	34
ESPECIFICACION.....	34
Ingresar al modo privilegiado	34
Switch>enable.....	34
Restaurar valores predeterminados	34
Switch#erase startup-config.....	34
Eliminar Vlan	34
Switch#delete vlan.dat	34
Reiniciar el Switch	34
Switch#reload.....	34
TAREA	35
ESPECIFICACION.....	35
Ingresar al modo privilegiado	35

Switch>enable.....	35
Active plantilla predeterminada	35
Switch#show sdm prefer	35
Habilitar plantilla SDM para IPV4 e IPV6.....	35
Switch#configure terminal	35
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default.....	35
Reiniciar el switch.....	35
Switch#reload.....	35
2.4.1.2 Paso 2: Configurar R1	36
2.4.1.3 Paso 3: Configure S1 y S2.....	42
2.5 Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)	46
2.5.1 Paso 4: Configurar S1.....	46
2.5.2 Paso 5: Configure el S2.....	50
2.6 Parte 3: Configurar soporte de host.....	53
2.6.1 Paso 1: Configure R1.....	53
2.6.2 Paso 2: Configurar los servidores	55
2.7 Parte 4: Probar y verificar la conectividad de extremo a extremo.....	57
CONCLUSIONES.....	63
BIBLIOGRAFIA	64
ANEXOS	66

LISTA DE TABLAS

Tabla 1 Esquema de direccionamiento	15
Tabla 2 Configuración R1	18
Tabla 3 Configuración S1	20
Tabla 4 Configuración PC A	23
Tabla 5 Configuración PC B	24
Tabla 6. Verificación conectividad	25
Tabla 7 Configuración tabla VLAN	31
Tabla 8 asignación de direcciones	31
Tabla 9 Eliminación configuración R1	33
Tabla 10 Inicialización y carga del Switch 1 y 2.....	34
Tabla 11 Configuración plantilla SDM en switch 1 y 2.....	35
Tabla 12 Configurar R1	36
Tabla 13 Configuración 2 R1	37
Tabla 14 Configure S1	42
Tabla 15 Configure 2 S1.....	43
Tabla 16 Configuración de la infraestructura de red.....	46
Tabla 17 Configuración 2 de la infraestructura de red.....	47
Tabla 18 Configuración el S2	50
Tabla 19 Configuración 2 el S2	51
Tabla 20 Configurar soporte de host	53
Tabla 21 configuración red PC-A	55
Tabla 22 Configurar los servidores.....	55
Tabla 23 configuración red PC-B	56
Tabla 24 comprobación conexiones.....	58
Tabla 25 comprobación conexiones.....	58

LISTA DE FIGURAS

Figura 1 Escenario 1	15
Figura 2 Simulación de escenario 1	15
Figura 3 calculo direccionamiento 60 Host.....	16
Figura 4 calculo direccionamiento 20 Host.....	17
Figura 5 comprobación configuración PC A	24
Figura 6 comprobación configuración PC B	25
Figura 7 Comprobación conexión PCA – R1 G0/0/0	26
Figura 8 Comprobación conexión PC A – R1 G0/0/1	27
Figura 9 Comprobación conexión PC A – S1 VLAN 1	27
Figura 10 Comprobación conexión PC A – PC B	28
Figura 11 Comprobación conexión PC B – R1 G 0/0	28
Figura 12 Comprobación conexión PC B – G0/0/1	29
Figura 13 Escenario 2	30
Figura 15 Borrado configuración Router.....	34
Figura 16 Borrado de configuración S1 Y S2	35
Figura 17 Verificación configuración SDM en S1 Y S2.....	36
Figura 22 Verificación ping PC-B N° 1.....	61
Figura 23 Verificación ping PC-B N° 2.....	62

GLOSARIO

ETHERCHANNEL:

Cuando se configura un EtherChannel, la interfaz virtual resultante se denomina “port channel” (canal de puertos). Las interfaces físicas se agrupan en una interfaz port channel, como se muestra en la figura.

¹

LAN:

LAN es la abreviatura de Local Area Network. Denomina redes con extensión física limitada.²

IPV4:

IPv4 es el nombre del protocolo de Internet utilizado actualmente para las direcciones IP de los dominios. Estas direcciones IP se asignan automáticamente cuando se registra un dominio.³

IPV6:

un nuevo protocolo con el que se generan nuevos tipos de direcciones IP más largos y complejos.⁴

Direccionamiento:

El direccionamiento es la configuración de la red de tal forma que a cada equipo le corresponde una única y exclusiva dirección, con el fin de que no haya errores a la hora de transmitir y recibir datos.⁵

Host:

La palabra inglesa host, que en español se traduciría como huésped, se usa en informática sobre todo a nivel de redes, donde en muchas ocasiones (no siempre), se asimila al concepto de servidor⁶.

Subnetting

Topología

La topología de red se representa normalmente mediante un dibujo de líneas y objetos que refleja la topología física y lógica general.⁷

¹ Ccnadesdecero.es, Funcionamiento de EtherChannel,

² Know How, LAN — Red de área local: la tecnología de un vistazo,(2020)

³ ionos.es, Qué es IPv4, (2022)

⁴ yúbal Fernández, IPv6: qué es, para qué sirve y qué ventajas tiene, (2019)

⁵ giret.ufps.edu.co, Direccionamiento,

⁶ sistemas.com, Definición de Host

⁷ arubanetworks.com, Qué es la topología de red,(2022)

Dominio:

dominio presenta dos acepciones, la primera es el conjunto de ordenadores conectados a una red y, uno de ellos administra a los usuarios y los privilegios que cada uno posee en la red. Por otra parte, es una dirección en la web, la misma se compone por: el nombre de la organización y el tipo de compañía, por ejemplo: .com, en referencia a este punto, lo más comunes son: .COM, .NET, .ORG.⁸

VTY:

Línea Terminal Virtual, En el router, los puertos vty están enumerados del 0 al 15 y son utilizados para establecer sesiones Telnet. El comando a utilizar es line vty 0 15 así como los subcomandos password y login.⁹

SSH

es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente¹⁰

RSA.

es un cifrado asimétrico que se utiliza en muchos ámbitos de la transmisión de datos en Internet por su facilidad de uso. Este sistema consta de una clave RSA pública y otra privada.¹¹

PING

es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión o host local. Mostramos sus usos.¹²

FIREWALL

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso.¹³

⁸ Significados.com, Significado de Dominio, (2022)

⁹ Liliana Rincón Valadez, Jesús Andrade Muñoz, Configurando un acceso administrativo seguro, (2009)

¹⁰ web.mit.edu, Protocolo SSH

¹¹ Ionos.es, Cómo funcionan las claves RSA, (2022)

¹² Tomás Ramírez, Qué es el comando Ping y cómo funciona, (2016)

¹³ idgrup.com, Qué es un Firewall,

RESUMEN

Se realiza la configuración de dos escenarios por medio de la plataforma Cisco en los cuales el estudiante debe realizar el enrutamiento adecuado para configurar la seguridad y los diversos parámetros de los dispositivos de conexión que tiene cada uno de ellos; en la configuración de dichos escenarios se debe investigar sobre direccionamiento IP en diferentes LAN para lograr configurar aspectos básicos de seguridad en las redes electrónicas propuestas.

Realizando la implementación de cada esquema y la configuración de cada uno de los dispositivos que tiene cada escenario, dando respuesta a cada problemática de configuración planteada por la guía de una forma única que es establecida por el estudiante, buscando la forma de configurar desde dispositivos hasta terminales e identificando que tipo de conexión se necesita para entablar conmutación entre dichos dispositivos; buscando dar una idea de los aspectos de seguridad que puede tener una red y lo importante que pueden llegar a ser, teniendo una verificación de conectividad entre lo elaborado, dándonos una idea de lo que puede ser una CCNA.

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

ABSTRACT

The configuration of two scenarios is carried out through the Cisco platform in which the student must carry out the appropriate routing to configure the security and the various parameters of the connection devices that each one of them has;

In the configuration of these scenarios, IP addressing in different LANs must be investigated in order to configure basic security aspects in the proposed electronic networks.

Carrying out the implementation of each scheme and the configuration of each one of the devices that each scenario has, responding to each configuration problem raised by the guide in a unique way that is established by the student, looking for a way to configure from devices to terminals and identifying what type of connection is needed to establish switching between said devices; seeking to give an idea of the security aspects that a network can have and how important they can be, having a connectivity verification between what has been prepared, giving us an idea of what a CCNA can be.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics

INTRODUCCIÓN

El desarrollo de este trabajo tiene como fin la identificación de comandos necesarios para la correcta configuración de ROUTERS, SWITCH y terminales las cuales darán unas bases óptimas para la configuración de una red simple en la cual el estudiante podrá dar conexión a varios equipos con distintos medios de comunicación y también establecer una seguridad optima en el proceso de la conexión de los usuarios.

En la primera red se establecerán cifrados de contraseñas creación de usuarios y parámetros definidos para las contraseñas que se utilizan en la configuración de la red también la identificación por medio de nombres establecidos a los equipos y a los dispositivos de conexión dentro de la red, también implementar y configurar mensajes de bienvenida y mensajes de error para los distintos ingresos al sistema.

En la segunda red se busca establecer una conexión por medio de la configuración IPV4 e IPV6 por medio de la configuración de ROUTERS, SWITCH para la conexión entre los pc. El enrutamiento de los dispositivos será configurado por medio de VLAN y DHCP al igual que ETHERCHANNEL y port-security

ESCENARIO 1

1.1 Escenario 1

Figura 1 Escenario 1



Fuente: Prueba de habilidades diplomado. CCNA

Figura 2 Simulación de escenario 1



Fuente: Prueba de habilidades diplomado. CCNA

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 1 Esquema de direccionamiento

Ítem	Requerimiento
Dirección de Red	172.84.3.0 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 172.84.3.62
R1 G0/0/0	Última dirección de host de la subred LAN2 172.84.3.94
S1 SVI	Segunda dirección de host de la subred LAN1 172.84.3.2
PC-A	Décima dirección de host de la subred LAN1 172.84.3.10
PC-B	Décima dirección de host de la subred LAN2 172.84.3.75

Fuente: Autor

1.2 CALCULO DIRECCIONAMIENTO IP

Figura 3 calculo direccionamiento 60 Host

CALCULAR MASCARA PARA 60 HOST									
IP	172,84,3,0								
CLASE IP	B								
MASCARA POR DEFECTO	255,255,255,0								
	255	255	255	0					
	11111111	11111111	11111111	00000000					
HOST 60	1	1	0	0	0	0	0	0	0
	128	64	32	16	8	4	2	1	
MASCARA PARA 60 HOST	255,255,255,192								
Nº TOTAL DE SUBREDES	2^N								
	$2^2 = 4$								
Nº TOTAL DE HOST	$2^N - 2$								
	$2^6 - 2 = 62$								
PRIMERA IP	172,84,3,1								
ULTIMA IP	172,84,3,62								
BROATCAST	172,84,3,63								

Fuente: Autor

Figura 4 calculo direccionamiento 20 Host

CALCULAR MASCARA PARA 60 HOST									
IP	172,84,3,64								
CLASE IP	B								
MASCARA POR DEFECTO	255,255,255,0								
	255	255	255	0					
	11111111	11111111	11111111	00000000					
HOST 20	1	1	1	0	0	0	0	0	0
	128	64	32	16	8	4	2	1	1
MASCARA PARA 60 HOST	255,255,255,224								
Nº TOTAL DE SUBREDES	2^N								
	$2^3 = 8$								
Nº TOTAL DE HOST	$2^N - 2$								
	$2^5 - 2 = 30$								
PRIMERA IP	172,84,3,65								
ULTIMA IP	172,84,3,94								
BROATCAST	172,84,3,95								

Fuente: Autor

En la figura 3 y 4 evidenciamos el proceso de cálculo del direccionamiento IP que se realiza para los distintos hosts establecidos.

Se procede a configurar cada uno de los dispositivos

Se asignan nombre y elementos de configuración de seguridad

1.3 CONFIGURACION ROUTER R1

1.3.1 ROUTER R1

Reuter>

Router>enable

Ingreso a modo privilegiado

Router#configure terminal

Ingreso a modo de configuración

Router(config)#hostname R1

Asigno nombre al router

R1(config)#interface s0/0

Configuro interfaz

serial 0R1(config-if) description to R2

R1(config-if) #ip address 10.103.12.1 255.255.255.0

Tabla 2 Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Enable Configure terminal No ir domain-lookup
Nombre del router	R1 Configure terminal Hostname R1
Nombre de dominio	ccna-sa.com` ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Enable password ciscoenpass Service password-encryption ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass Login
Establecer la longitud mínima para las contraseñas	Security passwords min-length 10 10 caracteres
Crear un usuario administrativo en la base	Nombre de usuario: admin

de datos local	<p>Contraseña: admin1pass</p> <p>Username admin password admin1pass</p>
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	<p>Line vty 0 15 Transport input ssh Login local</p>
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	<p>Line vty 0 5 Transport input ssh Login local</p>
Cifrar las contraseñas de texto no cifrado	<p>Service password-encryption</p>
Configurar un banner MOTD	<p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <p>Banner motd %ROUTER R1 CONFIGURADO POR FABIAN ANDRES LANCHEROS PINZON ESTUDIANTE DE INGENIERIA DE SISTEMAS%</p> <p>Exit</p> <p>Running-config startup-config</p>
Configuración de interface G0/0/0	<p>Establecer la descripción Establecer la dirección IPv4</p> <p>Activar la interfaz.</p>

	<p>Interface gigabitethernet 0/0 Ip address 172.84.3.94 255.255.255.224</p> <p>No shutdown</p>
Configuración de interface G0/0/1	<p>Establecer la descripción Establecer la dirección IPv4 Activar la interfaz.</p> <p>Interface gigabitethernet 0/0 Ip address 172.84.3.62 255.255.255.192</p> <p>No shutdown</p>
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Autor

1.4 CONFIGURACION S1

Tabla 3 Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS	<p>Enable</p> <p>Configure terminal</p> <p>No ir domain-lookup</p>
Nombre del switch	S1

	<p>Hostname s1</p>
<p>Nombre de dominio</p>	<p>ccna-sa.com</p> <p>ip domain-name ccna-sa.com</p>
<p>Contraseña cifrada para el modoEXEC privilegiado</p>	<p>Ciscoenpass</p> <p>Enable password ciscoenpass</p> <p>Service password-encryption</p>
<p>Contraseña de acceso a la consola</p>	<p>Ciscoconpass</p> <p>Line console 0</p> <p>Password ciscoconpass</p> <p>Login</p>
<p>Apagar todos los puertos sin usar</p>	<p>F0/1-4, F0/7-24, G0/1-2</p> <p>Interface range fasEthernet 0/1-4</p> <p>Shutdown</p> <p>Interface range fasEthernet 0/7-24</p> <p>shutdown</p> <p>Interface range.gigabitEthernet 0/1-2</p> <p>shutdown</p>
<p>Crear un usuario administrativo en la base de datos local</p>	<p>Nombre de usuario: admin</p> <p>Contraseña: admin1pass</p>

	Username admin password admin1pass Enable secret Ciscoenpass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Transport input ssh Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	ip ssh versión 2
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. Banner motd #S1 configurado por FABIAN ANDRES LANCHEROS PINZON estudiante de INGENIERIA DE SISTEMAS# Exit Copy running-config startup-config
Generar una clave de cifrado RSA	Módulo de 1024 bits Crypto key generate rsa 1024
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4 Configure terminal Interface vlan 1 Ip address 172.84.3.2 255.255.255.192

Fuente: Autor

Se realiza una configuración de seguridad del dispositivo en la cual se definen nombre contraseñas y seguridad para el usuario privilegiado igual forma la creación de un usuario, también realizamos la configuración de las interfaces que se van a utilizar y se habilita la versión ssh, deshabilitamos los puertos que no se utilizan y realizamos un servicio de encriptación de contraseña

1.5 CONFIGURACION DE LOS EQUIPOS

1.5.1 EQUIPO A

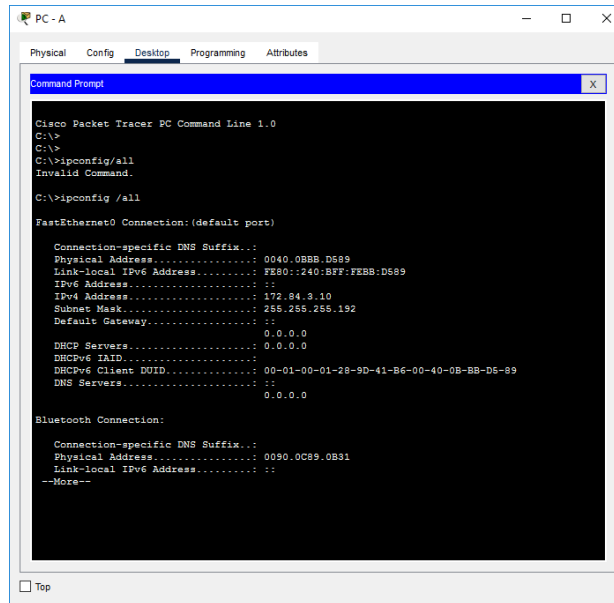
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 4 Configuración PC A

Configuración de red de PC-A	
Descripción	
Dirección física	0040.0bbb.d589
Dirección IPv4	172.84.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.84.3.0

Fuente: Autor

Figura 5 comprobación configuración PC A



Fuente: Autor

En la figura 5 podemos comprobar la configuración del dispositivo con el comando ipconfig /all el cual nos dice que ip tiene la maquina

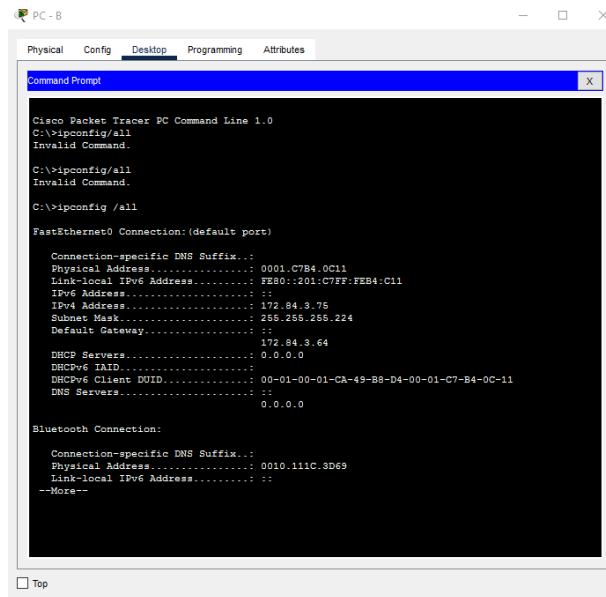
1.5.2 EQUIPO B

Tabla 5 Configuración PC B

Configuración de red de PC-B	
Descripción	
Dirección física	0001.c7b4.0c11
Dirección IPv4	172.84.3.75
Máscara de subred	75255.255.255.
Puerta de enlace IPv4 predeterminada	224172.84.3.64

Fuente: Autor

Figura 6 comprobación configuración PC B



Fuente: Autor

En la figura 6 podemos comprobar la configuración del dispositivo con el comando ipconfig /all el cual nos dice que ip tiene la maquina

Se realiza una configuración establecida a los equipos de cómputo y se verifica con que conectividad queda.

1.6 PROBAR Y VERIFICAR CONECTIVIDAD

Tabla 6. Verificación conectividad

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.84.3.94	Conexión exitosa
	R1 G0/0/1	172.84.3.62	Conexión exitosa

	S1 VLAN 1	172.84.3.2	Conexión exitosa
	PC-B	172.84.3.75	Conexión exitosa
PC-B	R1 G0/0/0	172.84.3.94	Conexión exitosa
	R1 G0/0/1	172.84.3.62	Conexión exitosa
	S1 VLAN1	172.84.3.2	Reques time out

Fuente: Autor

Se realiza una verificación por medio del comando ping a cada una de las ips configuradas en los distintos dispositivos de la red verificando que se establezca una conexión activa después de las configuraciones solicitadas.

1.6.1 DE PC-A A R1 G0/0/0

Figura 7 Comprobación conexión PCA – R1 G0/0/0

```

PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 172.84.3.84: bytes=32 time=1ms TTL=255
Ping statistics for 172.84.3.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms
C:\>ping 172.84.3.75

Pinging 172.84.3.75 with 32 bytes of data:

Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Ping statistics for 172.84.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>ping 172.84.3.94

Pinging 172.84.3.94 with 32 bytes of data:

Reply from 172.84.3.94: bytes=32 time=1ms TTL=255
Reply from 172.84.3.94: bytes=32 time=1ms TTL=255
Reply from 172.84.3.94: bytes=32 time=1ms TTL=255
Reply from 172.84.3.94: bytes=32 time=1ms TTL=255
Ping statistics for 172.84.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

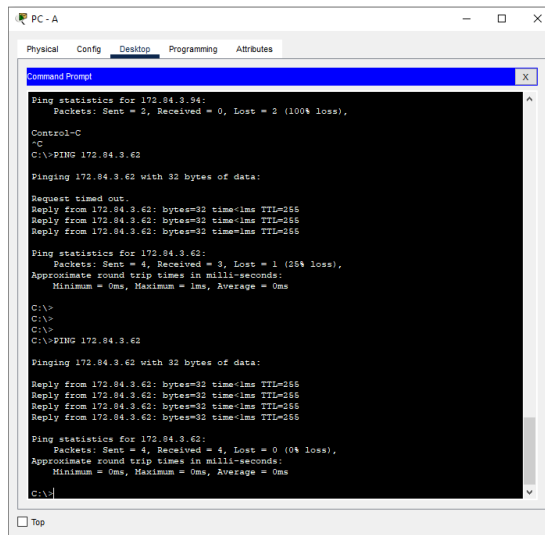
```

Fuente: Autor

En la figura 7 podemos observar la conexión exitosa por medio del ping a la IP asignada a R1

1.6.2 DE PC-A A R1 G0/0/1

Figura 8 Comprobación conexión PC A – R1 G0/0/1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 172.84.3.62:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\>PING 172.84.3.62

Pinging 172.84.3.62 with 32 bytes of data:
Request timed out.
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255

Ping statistics for 172.84.3.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
C:\>
C:\>
C:\>PING 172.84.3.62

Pinging 172.84.3.62 with 32 bytes of data:
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255
Reply from 172.84.3.62: bytes=32 time=1ms TTL=255

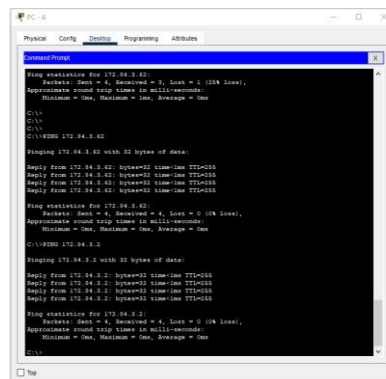
Ping statistics for 172.84.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autor

La figura 8 podemos observar la correcta conexión del PC-A al R1 por medio de la respuesta que nos da el ping a la ip configurada en R1 -G0/0/1

1.6.3 DE PC-A A S1 VLAN 1

Figura 9 Comprobación conexión PC A – S1 VLAN 1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 172.84.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
C:\>
C:\>
C:\>PING 172.84.3.2

Pinging 172.84.3.2 with 32 bytes of data:
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255

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

Pinging 172.84.3.2 with 32 bytes of data:
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255
Reply from 172.84.3.2: bytes=32 time=1ms TTL=255

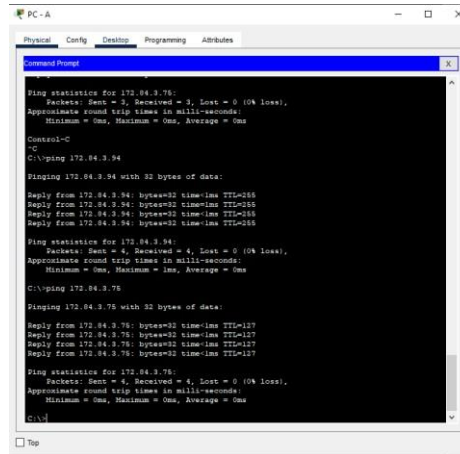
Ping statistics for 172.84.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Fuente: Autor

En la figura 9 se comprueba la correcta conexión por medio del comando PING de PC-A a la ip configurada en S1 VLAN 1

1.6.4 DE PC-A A PC-B

Figura 10 Comprobación conexión PC A – PC B



```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 172.84.3.75:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 172.84.3.94

Pinging 172.84.3.94 with 32 bytes of data:

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

Ping statistics for 172.84.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.84.3.75

Pinging 172.84.3.75 with 32 bytes of data:

Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127
Reply from 172.84.3.75: bytes=32 time=1ms TTL=127

Ping statistics for 172.84.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

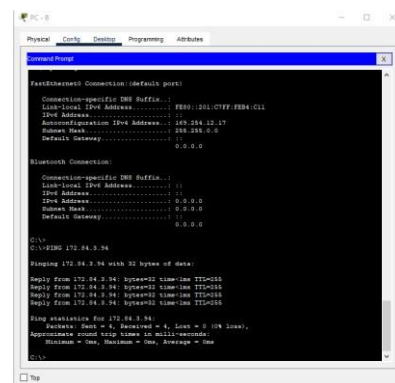
C:\>
```

Fuente Autor

En la figura 10 podemos comprobar por medio del PING realizado de PC-A a la ip configurada en PC-B que existe una conexión exitosa

1.6.5 De PC-B A R1 G 0/0

Figura 11 Comprobación conexión PC B – R1 G 0/0



```
PC - B
Physical Config Desktop Programming Attributes
Command Prompt
FastEthernet0/0 Connection (default port)
Connection-specific DNS Suffix...
Link-local IPv6 Address... FE80::151:C7FF:FE84:C11
IPv4 Address...
Subnet Mask... 255.255.255.0
Default gateway... 0.0.0.0

Ethernet0 Connection
Connection-specific DNS Suffix...
Link-local IPv6 Address...
IPv4 Address... 0.0.0.0
Subnet Mask... 0.0.0.0
Default gateway... 0.0.0.0

C:\>
C:\>ping 172.84.3.94

Pinging 172.84.3.94 with 32 bytes of data:

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

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

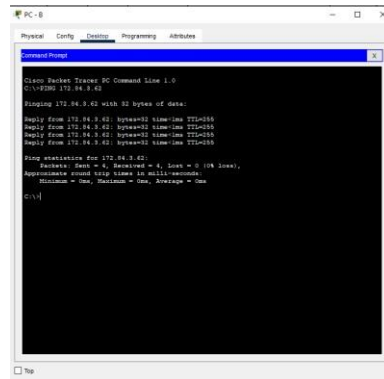
C:\>
```

Fuente Autor

En la figura 11 podemos comprobar la correcta conexión por medio del ping establecido entre PC-B y R1 G0/0

1.6.7 De PC-B A R1 G0/0/1

Figura 12 Comprobación conexión PC B – G0/0/1



```
PC-B
Physical Config Settings Programming Attributes
Command Prompt
C:\> Packet Tracer PC Command Line 1.0
C:\> PING 172.16.3.42
Pinging 172.16.3.42 with 32 bytes of data:
Reply from 172.16.3.42: bytes=32 time=1ms TTL=64
Reply from 172.16.3.42: bytes=32 time=1ms TTL=64
Reply from 172.16.3.42: bytes=32 time=1ms TTL=64
Reply from 172.16.3.42: bytes=32 time=1ms TTL=64
Ping statistics for 172.16.3.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

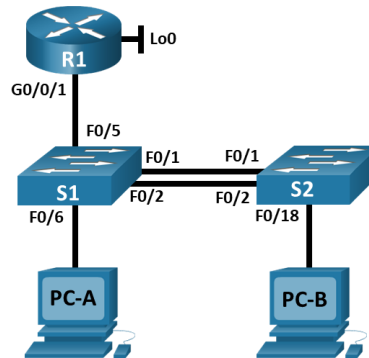
Fuente: Autor

En la figura 12 podemos comprobar la correcta conexión por medio del ping establecido entre PC-B y R1 G0/1

2. ESCENARIO 2

2.1 Escenario 2

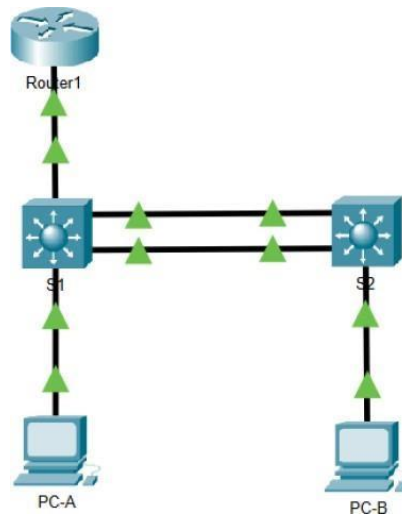
Figura 13 Escenario 2



Fuente: Prueba de habilidades diplomado. CCNA

2.2 Simulación del escenario 2

Figura 14 Simulación del escenario 2



Fuente: Prueba de habilidades diplomado. CCNA

2.3 CONFIGURACION

En este escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 7 Configuración tabla VLAN

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

Fuente: Autor

2.3.1 Asignación de direcciones

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberáemplazarlos 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	10.84.8.1 /26 255.255.255.192	No corresponde

	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.84.8.65 /27 255.255.255.224	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.84.8.97 /29 255.255.255.248	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 /27 255.255.255.224	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.84.8.98 /29 255.255.255.248	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.84.8.99 /29 255.255.255.248	10.19.8.97
	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 puerta de enlace predeterminada

	DHCP para dirección IPv4	IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Autor

2.4 INSTRUCCIONES ESCENARIO 2

2.4.1 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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

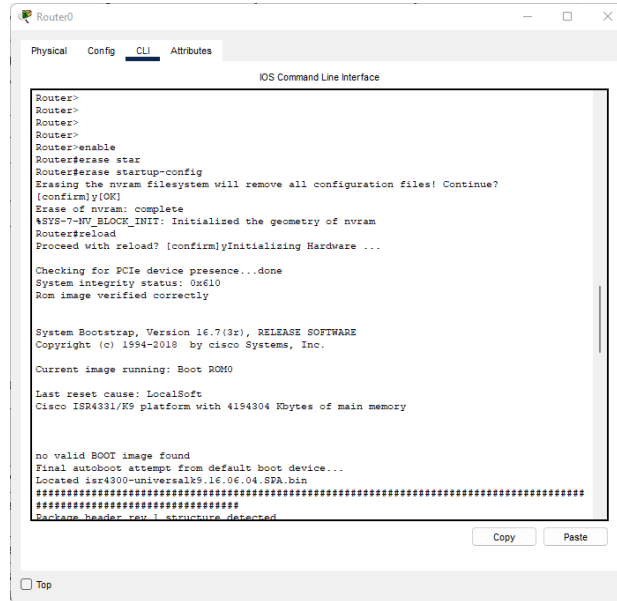
- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6según sea necesario y vuelva a cargar el switch.

Tabla 9 Eliminación configuración R1

TAREA	ESPECIFICACION
Ingresar al modo privilegiado	Router>enable
Restaurar valores predeterminados	Router#erase startup-config
Reiniciar el Router	Router#reload

Fuente: Autor

Figura 145 Borrado configuración Router



Fuente: Autor

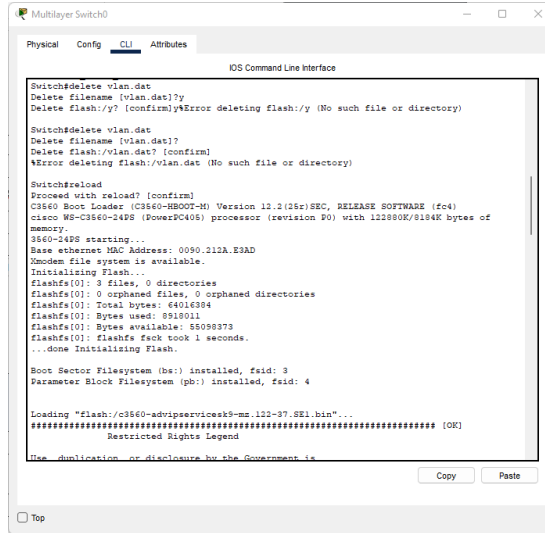
En la figura 15 Ingresamos al router por medio de la consola con permisos de usuario privilegiado y procedemos a eliminar la configuración que tiene definida bajo el comando erase startup-config el cual borra el contenido almacenado en la NVRAM después reiniciamos el router para que la configuración quede establecida.

Tabla 10 Inicialización y carga del Switch 1 y 2

TAREA	ESPECIFICACION
Ingresar al modo privilegiado	Switch>enable
Restaurar valores predeterminados	Switch#erase startup-config
Eliminar Vlan	Switch#delete vlan.dat
Reiniciar el Switch	Switch#reload

Fuente: Autor

Figura 156 Borrado de configuración S1 Y S2



Fuente: Autor

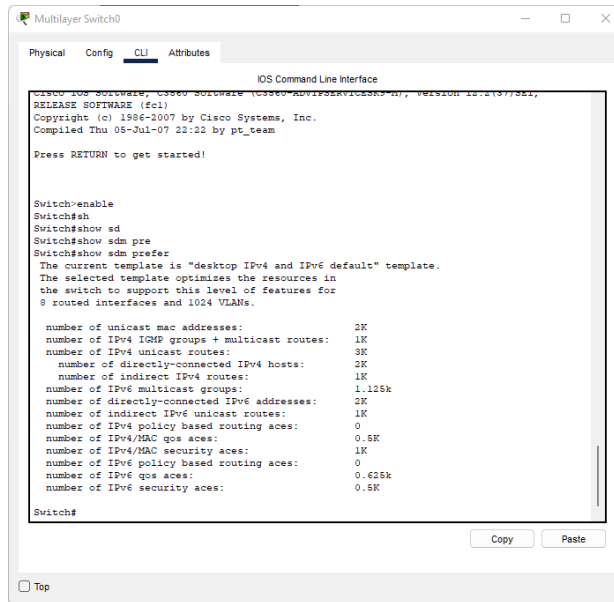
En la figura 16 se ingresa a los dos dispositivos S1 y S2 a través de la consola en el modo privilegiado para ejecutar el comando erase startup-config el cual borrara el contenido de la NVRAM luego eliminamos el archivo de configuración de la VLAN con el comando delete vlan.dat y pasamos a reiniciar los dispositivos para que tomen los cambios.

Tabla 11 Configuración plantilla SDM en switch 1 y 2

TAREA	ESPECIFICACION
Ingresar al modo privilegiado	Switch>enable
Active plantilla predeterminada	Switch#show sdm prefer
Habilitar plantilla SDM para IPV4 e IPV6	Switch#configure terminal Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Reiniciar el switch	Switch#reload

Fuente: Autor

Figura 167 Verificación configuración SDM en S1 Y S2



Fuente: Autor

Debido a que el Switch seleccionado no soporta IPV6 se configura la plantilla SDM para que lo admita IPV4 e IPV6 desde el modo privilegiado se activa la plantilla predeterminada y se configura el dual de IPV4 e IPV6 luego se procede a realizar el reinicio del dispositivo para que los cambios queden guardados, se verifica con el comando show sdm prefer

2.4.1.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12 Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router	R1 Router(config)#hostname R1

Nombre de dominio	ccna-sa.com R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Class R1(config)#enable secret Class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line) #password Cisco R1(config-line) #login R1(config-line) #exit
Establecer la longitud mínima para las contraseñas	Security passwords min-length 5 R1(config)#security passwords min-length 5
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass R1(config)#username admin password 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	R1(config-line) #transport input ssh R1(config-line) #exit

Fuente: Autor

Tabla 13 Configuración 2 R1

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	<p>Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> <pre>R1(config)#Banner motd %ROUTER S1 CONFIGURADO POR FABIAN ANDRES LANCHEROS PINZON ESTUDIANTE DE INGENIERIA DE SISTEMAS% Exit</pre>
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	<p>Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80::1 Establece la dirección IPv6 Activar la interfaz.</p> <pre>R1(config)#interface gigabitEthernet 0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description vlan Docentes R1(config-subif)#ip address 10.84.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local</pre>

	<pre> R1(config-subif)#interface gigabitEthernet 0/0/1.30 R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description vlan Estudiantes R1(config-subif)#ip address 10.84.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface gigabitEthernet 0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description vlan Invitados R1(config-subif)#ip address 10.84.8.97 255.255.255.248 R1(config-subif)#ip address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#interface gigabitEthernet 0/0/1.56 R1(config-subif)#encapsulation dot1q 56 </pre>
--	--

	<pre> 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>
<p>Configure el Loopback0 interface</p>	<pre> Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 ip address 209.165.201.1 255.255.255.224 ipv6 address 2001:db8:acad:209::1/64 ipv6 address fe80::1 link-local no shutdown exit 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 </pre>

	R1(config-if)#exit
Generar una clave de cifrado RSA	<p>Módulo de 1024 bits</p> <pre>crypto key generate rsa general-keys modulus 1024</pre> <p>R1(config)#crypto key generate rsa</p> <p>The name for the keys will be: R1.ccna-sa.com</p> <p>Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]:</p> <p>1024</p> <p>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p>

Fuente: Autor

Se realiza la configuración del router R1 configuración como el nombre la definición del Dominio y establecer la contraseña cifrada en el modo EXEC privilegiado también se define el usuario administrativo y contraseña se realiza la activación de rutin IPV6 para poder definir en la interfaz de conexión que configuración ipv6 e ipv4 se le define a casa interfaz también se agrupan por VLAN y se le asigna a cada uno su configuración IPV6 y

4. Revisamos su configuración con el comando show running-config.

2.4.1.3 Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 14 Configure S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	S1 o S2, según proceda Switch(config)#hostname S1 Switch(config)#hostname S2
Nombre de dominio	ccna-sa.com S1(config)#ip domain-name ccna-sa.com S2(config)#ip domain name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Class S1(config)#enable secret Class S2(config)#enable secre Class
Contraseña de acceso a la consola	Cisco S1(config)#line console 0 S1(config-line)#password Cisco S1(config-line)#login

	S1(config-line)#exit 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	Nombre de usuario: admin Password: admin1pass S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass

Fuente: Autor

Tabla 15 Configure 2 S1

Tarea	Especificación
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 S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.

<p>Configurar un MOTD Banner</p>	<p>S1(config)#banner motd %Swicht S1 configurado por Fabian Andres Lancheros Pinzon estudiante de Ingeniería de sistemas%</p> <p>S2(config)#banner motd %Swicht S1 configurado por Fabian Andres Lancheros Pinzon estudiante de Ingeniería de sistemas%</p>
<p>Generar una clave de cifrado RSA</p>	<p>Módulo de 1024 bits</p> <p>crypto key generate rsa general-keys modulus 1024</p> <p>S1(config)#crypto key generate rsa</p> <p>The name for the keys will be: S1.ccnasa.com</p> <p>Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]: 1024</p> <p>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p> <p>S2(config)#crypto key generate rsa</p> <p>The name for the keys will be: S2.ccnasa.com</p> <p>Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take</p>

	<p>a few minutes.</p> <p>How many bits in the modulus [512]: 1024</p> <p>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p>
<p>Configurar la interfaz de administración (SVI)</p>	<p>Establecer la dirección IPv4 de capa3</p> <p>Establezca la dirección local de enlace IPv6 como FE80: :98 para S1y FE80: :99 para S2</p> <p>Establecer la dirección IPv6 de capa3</p> <p>S1(config)#interface vlan 4</p> <p>S1(config-if)#ip address 10.84.8.98 255.255.255.248</p> <p>S1(config-if)#ipv6 address 2001:db8:acad:c::98/64</p> <p>S1(config-if)#ipv6 address fe80::98 link-local</p> <p>S1(config-if)#description vlan administrador</p> <p>S1(config-if)#no shutdown</p> <p>S2(config)#interface vlan 4</p> <p>S2(config-if)#ip address 10.84.8.99 255.255.255.248</p> <p>S2(config-if)#ipv6 address 2001:db8:acad:c::99/64</p> <p>S2(config-if)#ip address fe80::99 link-local</p> <p>S2(config-if)#description vlan administrador</p> <p>S2(config-if)#no shutdown</p>

Configuración del gateway predeterminado	<p>Configure la puerta de enlace predeterminada como 10.XY.8.97 para IPv4</p> <pre>S1(config)#ip default-gateway 10.84.8.97 S2(config)#ip default-gateway 10.84.8.97</pre>
--	---

Fuente: Autor

Se realiza la respectiva configuración a cada Switch donde se establece la puerta de enlace la contraseña cifrada y el banner configuramos la IPV 4 y 6 para la interfaz vlan 4 y se define el módulo a 124 bits en los dos dispositivos

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

2.5.1 Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 16 Configuración de la infraestructura de red

Tarea	Especificación
Crear VLAN	<p>VLAN 20, nombre Docentes</p> <p>VLAN 30, nombre Estudiantes</p> <p>VLAN 40, nombre</p>

	Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#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
--	--

Fuente: Autor

Tabla 17 Configuración 2 de la infraestructura de red

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6nativa	Interfaces F0/1, F0/2 y F0/5 S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk

	<pre> S1(config-if)#switchport trunk native vlan 56 S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56 </pre>
<p>Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2</p>	<p>Usar el protocolo LACP para la negociación</p> <pre> S1(config)#interface range fastEthernet 0/1-2 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 trunk native 56 </pre>
<p>Configurar el puerto de acceso de host paraVLAN 2</p>	<pre> Interface F0/6 S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20 </pre>

Configurar la seguridad del puerto en lospuertos de acceso	Permitir 4 direcciones MAC S1(config-if)#switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar S1(config)#interface range fa 0/3-4 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description INHABILITADAS S1(config-if-range)#shutdown S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description INHABILITADAS S1(config-if-range)#shutdown S1(config-if-range)#interface range g 0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description INHABILITADAS S1(config-if-range)#shutdown

Fuente: Autor

Se ingresa al dispositivo y se realiza la configuración de las Vlan asignándolas según la tabla establecida por la guía. Se configuran las interfaces cuando los puertos para etherchannel de capa 2 utilizando el protocolo LACP también se des activan todas las interfaces que no se utilizan dejando un mensaje de inhabilitadas y también ingresándolas a la misma vlan

2.5.2 Paso 5: Configure el S2.

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

Tabla 18 Configuración el S2

Tarea	Especificación
<p>Crear VLAN</p>	<p>VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native</p> <pre>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</pre>
<p>Crear troncos 802.1Q que utilicen la VLAN 6nativa</p>	<p>Interfaces F0/1 y F0/2</p> <pre>S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#shutdown</pre>

	<pre>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>
<p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p>	<pre>Usar el protocolo LACP para lanegociación 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>
<p>Configurar el puerto de acceso del host para la VLAN 3</p>	<pre>Interfaz F0/18 S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30</pre>

Fuente: Autor

Tabla 19 Configuración 2 el S2

Tarea	Especificación
<p>Configure port-security en los access ports</p>	<pre>permite 4 MAC addresses S2(config-if)#switchport port-security maximum 4</pre>

<p>Asegure todas las interfaces no utilizadas.</p>	<p>Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar</p> <pre> 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 INHABILITADA S2(config-if-range)#shutdown S2(config)#interface range fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description INHABILITADA S2(config-if-range)#shutdown </pre>
--	---

Fuente: Autor

Después de realizar las respectivas configuraciones a los puertos que se van a utilizar y deshabilitar los puertos que no se van a utilizar des activándolos y asignándoles la misma vlan procedemos a dejar un máximo de 4 accesos al switch también nombramos las vlan según la tabla asignada por la guía y procedemos a encender los puertos Fa 1 y 2 en los dos dispositivos con el comando no shutdown

2.6 Parte 3: Configurar soporte de host

2.6.1 Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 20 Configurar soporte de host

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 quedirijan el tráfico a la interfaz Loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por lasúltimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net yespecifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

	<pre> R1(config)#ip dhcp excluded-address 10.84.8.1 10.84.8.52 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config)#network 10.84.8.0 255.255.255.192 R1(dhcp-config)#default-route 10.84.8.1 R1(dhcp-config)#domain-name unad-ccna- sa.net R1(dhcp-config)#exit </pre>
<p>Configurar DHCP IPv4 para VLAN 3</p>	<p>Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente.</p> <p>Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p> <pre> R1(config)#ip dhcp excluded-address 10.84.8.65 10.84.8.84 R1(config)#ip dhcp pool vlan30-estudiantes R1(dhcp-config)#network 10.84.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.84.8.65 R1(dhcp-config)#domain-name unad-ccna- sb.net R1(dhcp-config) </pre>

Fuente: Autor

Se procede a realizar la configuración de las rutas de una forma predeterminada en IPV4 e IPV6 las cuales realizaran un direccionamiento a la interfaz Loopback 0 estableciendo las rutas para conectar a internet. La configuración del DHCP para IPV4 en la VLAN20 se establece mediante las 10 últimas direcciones de la subred la cual está en el rango 10.84.8.1 a la 10.84.8.52 y la configuración de la VLAN 3 bajo las direcciones de 10.84.8.65 a la 10.84.8.84 también se define el nombre de dominio unad-ccna-sb.net

2.6.2 Paso 2: Configurar los servidores

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

Tabla 21 configuración red PC-A

Configuración de red de PC-A	
Descripción	Configurada por dhcp conectada a S1
Dirección física	

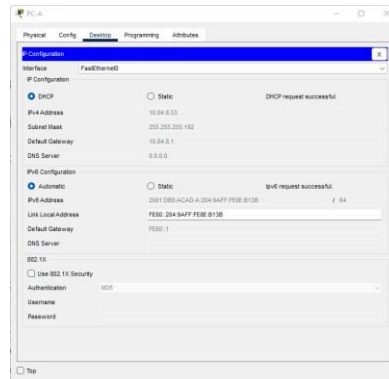
Fuente: Autor

Tabla 22 Configurar los servidores

Configuración de red de PC-A	
Dirección IP	10.84.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.84.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Figura 18 Verificamos la conexión PC-A



Fuente: Autor

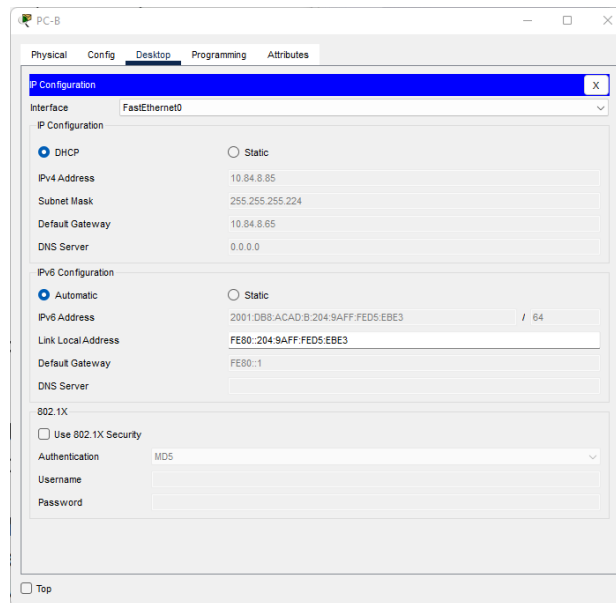
En la figura 18 podemos evidenciar la configuración estipulada al dispositivo PC-A por medio del DHCP el cual asigna la configuración debido a la configuración asignada a S1 y R1

Tabla 23 configuración red PC-B

Configuración de red de PC-B	
Descripción	Configurado por DHCP conectado a S2
Dirección física	
Dirección IP	10.84.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.84.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Figura 19 Verificamos la Configuración PC-B



Fuente: Autor

En la figura 19 se realiza la configuración de los equipos de cómputo por DHCP para que establezca la configuración realizada a los dispositivos de conexión. Permitiendo que el R1 y los S1-S2 realicen su configuración por medio de los parámetros DHCP configurados.

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

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 24 comprobación conexiones

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.84.8.1	Conexión exitosa
		IPv6	2001:db8:acad:a::1	Conexión exitosa
	R1, G0/0/1.30	IPv4	10.84.8.65	Conexión exitosa
		IPv6	2001:db8:acad:b::1	Conexión exitosa
	R1, G0/0/1.40	IPv4	10.84.8.97	Conexión exitosa
		IPv6	2001:db8:acad:c::1	Conexión exitosa
	S1, VLAN 40	IPv4	10.84.8.98	Conexión exitosa
		IPv6	2001:db8acad:c::98	

Fuente: Autor

Tabla 25 comprobación conexiones

Desde	A		Dirección IP	Resultados de ping
	S2, VLAN 40	IPv4	10.84.8.99	Conexión exitosa
		IPv6	2001:db8:acad:c::98	
	PC-B	IPv4	10.84.8.85	Conexión exitosa
		IPv6	2001:DB8:ACAD:B:204:9AFF:FED5:EBE3	Conexión exitosa
	R1 Bucle 0	IPv4	209.165.201.1	Conexión exitosa
		IPv6	2001:db8:acad:209::1	Conexión exitosa
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Conexión exitosa

	IPv6	2001:db8:acad:209::1	Conexión exitosa
R1, G0/0/1.2	IPv4	10.84.8.1	Conexión exitosa
	IPv6	2001:db8:acad:a::1	Conexión exitosa
R1, G0/0/1.3	IPv4	10.84.8.65	Conexión exitosa
	IPv6	2001:db8:acad:b::1	Conexión exitosa
R1, G0/0/1.4	IPv4	10.84.8.97	Conexión exitosa
	IPv6	2001:db8:acad:c::1	Conexión exitosa
S1, VLAN 4	IPv4	10.84.8.98	Conexión exitosa
	IPv6	2001:db8:acad:c::98	
S2, VLAN 4	IPv4	10.84.8.99	Conexión exitosa
	IPv6	2001:db8:acad:c::98	

Fuente: Autor

Figura 20 Verificación ping PCA N° 1

```

C:\>ping 10.84.8.1

Pinging 10.84.8.1 with 32 bytes of data:

Reply from 10.84.8.1: bytes=32 time=1ms TTL=255
Reply from 10.84.8.1: bytes=32 time=1ms TTL=255
Reply from 10.84.8.1: bytes=32 time=1ms TTL=255
Reply from 10.84.8.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.84.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 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:\>ping 10.84.8.65

Pinging 10.84.8.65 with 32 bytes of data:

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

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

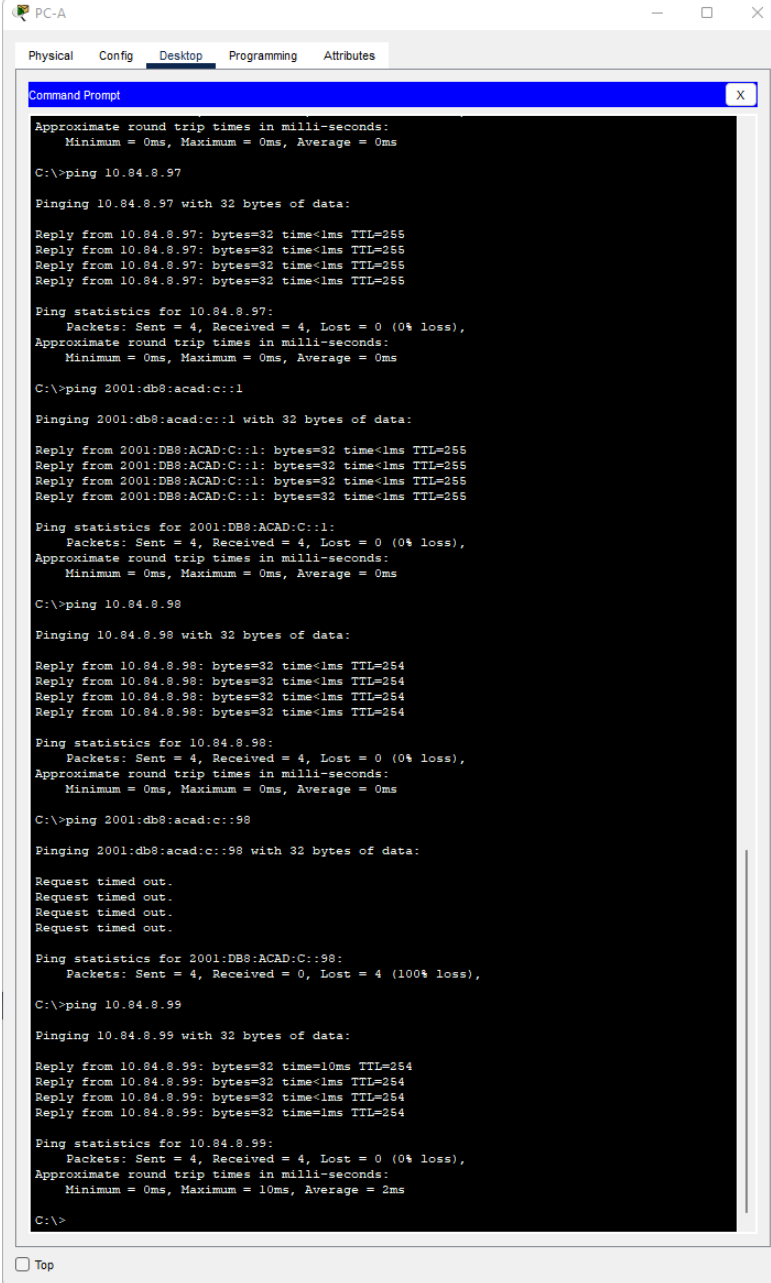
Ping statistics for 2001:db8:acad:b::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Fuente: Autor

En la figura 20 se evidencia la exitosa conexión por medio del comando PING a las

distintas configuraciones IP de los dispositivos de la red, dichas direcciones se configuran de acuerdo a la tabla de direccionamiento establecida por la guía.

Figura 21 Verificación ping PCA N° 2



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.84.8.97

Pinging 10.84.8.97 with 32 bytes of data:

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

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

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

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

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

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

C:\>ping 10.84.8.98

Pinging 10.84.8.98 with 32 bytes of data:

Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254
Reply from 10.84.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.84.8.98:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.84.8.99

Pinging 10.84.8.99 with 32 bytes of data:

Reply from 10.84.8.99: bytes=32 time=10ms TTL=254
Reply from 10.84.8.99: bytes=32 time<1ms TTL=254
Reply from 10.84.8.99: bytes=32 time<1ms TTL=254
Reply from 10.84.8.99: bytes=32 time<1ms TTL=254

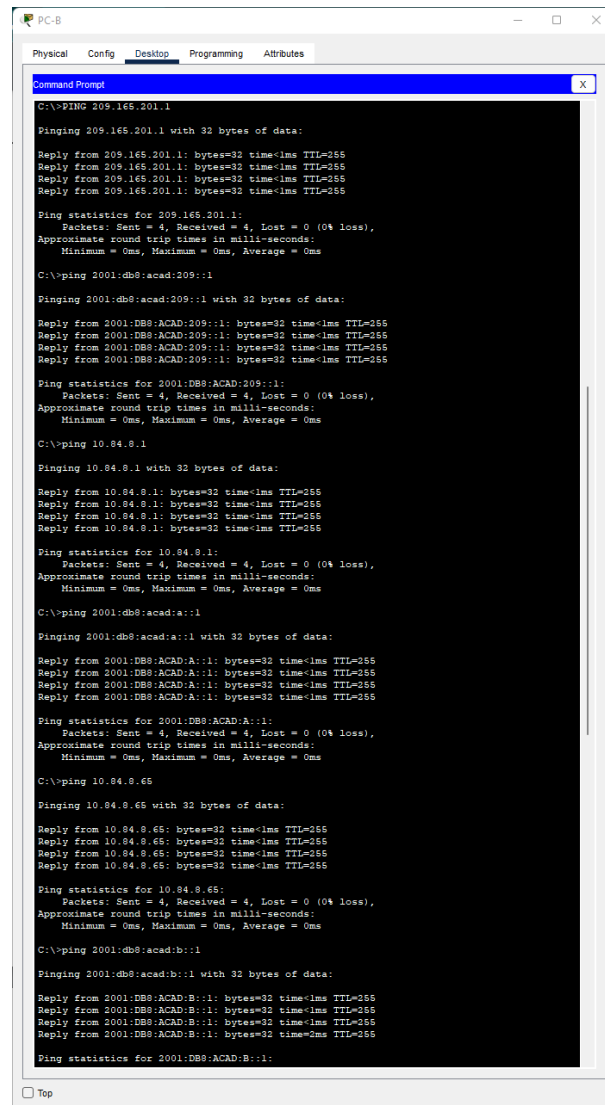
Ping statistics for 10.84.8.99:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

Fuente: Autor

En la figura 21 se evidencia la exitosa conexión por medio del comando PING a las distintas configuraciones IP de los dispositivos de la red, dichas direcciones se configuran de acuerdo a la tabla de direccionamiento establecida por la guía.

Figura 172 Verificación ping PC-B N° 1



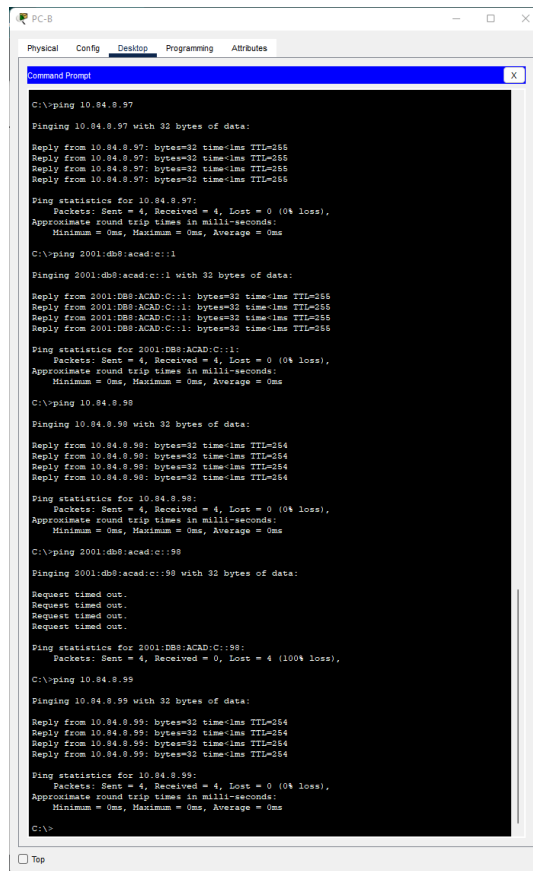
```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>PING 209.165.201.1
Pinging 209.165.201.1 with 32 bytes of data:
Reply from 209.165.201.1: bytes=32 time<ms TTL=255
Reply from 209.165.201.1: bytes=32 time<ms TTL=255
Reply from 209.165.201.1: bytes=32 time<ms TTL=255
Reply from 209.165.201.1: bytes=32 time<ms TTL=255
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db8:acad:209::1
Pinging 2001:db8:acad:209::1 with 32 bytes of data:
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<ms TTL=255
Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.84.8.1
Pinging 10.84.8.1 with 32 bytes of data:
Reply from 10.84.8.1: bytes=32 time<ms TTL=255
Reply from 10.84.8.1: bytes=32 time<ms TTL=255
Reply from 10.84.8.1: bytes=32 time<ms TTL=255
Reply from 10.84.8.1: bytes=32 time<ms TTL=255
Ping statistics for 10.84.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 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<ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<ms 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 10.84.8.65
Pinging 10.84.8.65 with 32 bytes of data:
Reply from 10.84.8.65: bytes=32 time<ms TTL=255
Reply from 10.84.8.65: bytes=32 time<ms TTL=255
Reply from 10.84.8.65: bytes=32 time<ms TTL=255
Reply from 10.84.8.65: bytes=32 time<ms TTL=255
Ping statistics for 10.84.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 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<ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<ms 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
 Top
```

Fuente: Autor

En la figura 22 se evidencia la exitosa conexión por medio del comando PING a las

distintas configuraciones IP de los dispositivos de la red, dichas direcciones se configuran de acuerdo a la tabla de direccionamiento establecida por la guía.

Figura 183 Verificación ping PC-B N° 2



```
C:\>ping 10.84.8.57

Pinging 10.84.8.57 with 32 bytes of data:

Reply from 10.84.8.57: bytes=32 time<ms TTL=255
Reply from 10.84.8.57: bytes=32 time<ms TTL=255
Reply from 10.84.8.57: bytes=32 time<ms TTL=255
Reply from 10.84.8.57: bytes=32 time<ms TTL=255

Ping statistics for 10.84.8.57:
    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<ms TTL=255
Reply from 2001:db8:acad:c::1: bytes=32 time<ms TTL=255
Reply from 2001:db8:acad:c::1: bytes=32 time<ms TTL=255
Reply from 2001:db8:acad:c::1: bytes=32 time<ms TTL=255

Ping statistics for 2001:db8:acad:c::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.84.8.98

Pinging 10.84.8.98 with 32 bytes of data:

Reply from 10.84.8.98: bytes=32 time<ms TTL=254
Reply from 10.84.8.98: bytes=32 time<ms TTL=254
Reply from 10.84.8.98: bytes=32 time<ms TTL=254
Reply from 10.84.8.98: bytes=32 time<ms TTL=254

Ping statistics for 10.84.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:db8:acad:c::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.84.8.99

Pinging 10.84.8.99 with 32 bytes of data:

Reply from 10.84.8.99: bytes=32 time<ms TTL=254
Reply from 10.84.8.99: bytes=32 time<ms TTL=254
Reply from 10.84.8.99: bytes=32 time<ms TTL=254
Reply from 10.84.8.99: bytes=32 time<ms TTL=254

Ping statistics for 10.84.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente Autor

En la figura 23 se evidencia la exitosa conexión por medio del comando PING a las distintas configuraciones IP de los dispositivos de la red, dichas direcciones se configuran de acuerdo a la tabla de direccionamiento establecida por la guía.

CONCLUSIONES

La configuración de una red en packet tracer permite definir aspectos importantes como la seguridad de un dispositivo permitiendo colocar varios protocolos que aseguran que la información estará protegida logrando así tener la seguridad de que todo se encontrará en óptimas condiciones.

Se puede tener la facilidad de crear diversos tipos de red sin importar lo complejo que sean, permitiendo realizar configuraciones de alto nivel y logrando comprobar el estado de los dispositivos conectados a las redes que se crean simulando conexiones de red local y de internet.

Finalmente, las configuraciones de los dispositivos nos permiten tener control total en cuando a dispositivos conectados, si deseamos que sean un número determinado para que no se exceda de un número definido por el creador de la red; de igual forma también permite tener un control total en cuando al tipo de configuración que puede tener la red estableciendo que configuración tiene cada uno gracias a una configuración DHCP.

BIBLIOGRAFIA

ASIGNAR NOMBRE de host de dispositivo en switches gestionados serie 300 mediante la interfaz de línea de comandos [Anónimo]. Cisco [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb1388-assign-device-host-name-on-300-series-managed-switches-using.html

CÓMO CONFIGURAR Consola en Cisco - CCNA Desde Cero [Anónimo]. CCNA Desde Cero [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

<https://ccnadesdecero.com/curso/configurar-consola-cisco/>

CÓMO CONFIGURAR Telnet en Cisco - CCNA Desde Cero [Anónimo]. CCNA Desde Cero [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

<https://ccnadesdecero.com/curso/como-configurar-telnet-en-cisco/#:~:text=Configurando%20la%20contraseña%20para%20Telnet,vty%20utilizando%20una%20contraseña%20simple.>

CONFIGURAR UN Servidor DHCP IPv4 [Anónimo]. WatchGuard Technologies | Network Security, Secure Wi-Fi, MFA, and Endpoint Security Solutions [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/configure_dhcp_server_c.html

CREAR USUARIOS en switches Cisco | nosololinux [Anónimo]. nosololinux [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

<https://nosololinux.es/crear-usuarios-en-switches-cisco/>

Networking, Cloud, and Cybersecurity Solutions - Cisco [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

https://www.cisco.com/c/es_mx/support/docs/ip/domain-name-system-dns/24182-reversedns.pdf

Redes [página web]. [Consultado el 27, noviembre, 2022]. Disponible en Internet:

<https://redesindex.webcindario.com/tema70.html#:~:text=Para%20borrar%20el%20archivo%20de,nvram%20filesystem%20will%20remove%20all>

ANEXOS

ANEXO A – Descarga de archivos de simulación

Enlace:

<https://drive.google.com/drive/folders/1gGgW7sVyC0JDuAyJre0W76wHmWgFT-Ezo?usp=sharing>