

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

MANUEL EDUARDO CUJABAN HURTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DUITAMA – BOYACÁ

2022

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

MANUEL EDUARDO CUJABAN HURTADO

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

DIRECTOR:

MSc. HECTOR JULIAN PARRA MOGOLLÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DUITAMA – BOYACÁ

2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Duitama, 30 de junio de 2022

AGRADECIMIENTOS

A Dios primeramente por sus bendiciones y a mi madre que impulso mis sueños y mis metas sin importar las dificultades y que siempre ha sido mi guía y ejemplo de lucha a quien dedico este gran logro.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	8
LISTA DE FIGURAS	10
GLOSARIO.....	11
RESUMEN.....	13
ABSTRACT	14
KEYWORDS.....	14
INTRODUCCIÓN.....	15
ESCENARIO 1	16
Parte 1: Construya la Red	16
Parte 2: Desarrolle el esquema de direccionamiento IP	17
Tabla de direccionamiento.....	17
Parte 3: Configure aspectos básicos R1 y S1.....	17
Las tareas de configuración para R1 incluyen las siguientes	17
Las tareas de configuración para S1.....	21
Paso 2. Configurar los equipos	23
PC-A Network Configuration	23
PC-C Network Configuración	24
PRUEBA DE CONECTIVIDAD	26
PCA A CON DESTINO A PC B	26
PC C CON DESTINO A PC A	27
ESCENARIO 2	28
Parte 2: Configurar los parámetros básicos de los dispositivos Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):.....	29
Paso 2: Configurar R1	30
Paso 3: Configurar R2.....	31
Paso 4: Configurar R3.....	34
Paso 5: Configurar S1	36

Paso 6: Configurar el S3	36
Paso 7: Verificar la conectividad de la red.....	37
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN	40
Paso 1: Configurar S1	40
Paso 2: Configurar el S3	42
Paso 3: Configurar R1	43
Paso 4: Verificar la conectividad de la red	44
Parte 4: Configurar el protocolo de routing dinámico OSPF	47
Paso 1: Configurar OSPF en el R1	47
Paso 2: Configurar OSPF en el R2.....	47
Paso 3: Configurar OSPFv3 en el R2	48
Paso 4: Verificar la información de OSPF	48
Parte 5: Implementar DHCP y NAT para IPv4.....	53
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	53
Paso 2: Configurar la NAT estática y dinámica en el R2.....	53
Paso 3: Verificar el protocolo DHCP y la NAT estática	55
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pingsse realicen.....	55
COMPROBACION DE CONECTIVIDAD	56
Parte 6: Configurar NTP.....	60
Parte 7: Configurar y verificar las listas de control de acceso (ACL)	60
Paso 1: Restringir el acceso a las líneas VTY en el R2.....	60
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 61	
Fuente propia.....	63
CONCLUSIONES	66
BIBLIOGRAFÍA.....	67
CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y	67
Conmutación, https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#7	67
CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y.....	67
Conmutación, https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#5	67

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos.	67
Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#10	67
CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación, https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#8	67
CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación, https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9	67
CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación, https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#6	67
CISCO. Principios básicos de routing y switching, https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#7.1.1.1	67
CISCO. Principios básicos de routing y switching, https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#6.1	67

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento	17
Tabla 2. Tabla Configuración R1	18
Tabla 3. Tabla Configuración s1	21
Tabla 4. Configuración PC A.....	23
Tabla 5. Configuración PC C	24
Tabla 6. Iniciar dispositivos	29
Tabla 7. Parámetros básicos de los dispositivos.....	29
Tabla 8. Configuración R1	30
Tabla 9. Configuración R2	31
Tabla 10. Configuración R3	34
Tabla 11. Configuración S1.....	36
Tabla 12. Configuración S3.....	37
Tabla 13. Verificación mediante ping	38
Tabla 14. Configuración de VLAN en S1	41
Tabla 15. Configuración S3.....	42
Tabla 16. Configuración R1	43
Tabla 17. Comprobación de conectividad	44
Tabla 18 .Configuración OSFP en R1.....	47
Tabla 19 .Configuración OSFP en R2.....	47
Tabla 20.Configuración OSFP V3 en R2	48
Tabla 21 .Verificación OSPF.....	49
Tabla 22. Configuración DHCP y VLAN en R1	53
Tabla 23.Configuración de NAT en R2	54
Tabla 24. Comprobación de conectividad DHCP y NAT	55
Tabla 25. Configuración NTP.....	60
Tabla 26. Configuración líneas VTY en R2	60

Tabla 27. Verificación de configuración 61

LISTA DE FIGURAS

Figura 1: Topología escenario 1	16
Figura 2. Configuración PCA	23
Figura 3. Configuración PC C	25
Figura 4. Prueba de conectividad PCA	26
Figura 5. Prueba de conectividad PC C	27
Figura 6. Topología de red escenario 2	28
Figura 7. Desde R1 A R2	38
Figura 8. Desde R2 A R3.....	39
Figura 9 .Desde PCA Gateway	40
Figura 10.Ping SW3 A VLAN 99 Y 21	45
Figura 11.Ping SW32 A VLAN 99 Y 21	46
Figura 12. Comprobación de configuración OSPF S1	50
Figura 13. Comprobación de configuración OSPF S2	51
Figura 14. Comprobación de configuración OSPF S3	52
Figura 15. Configuración DHCP PCA	56
Figura 16. Configuración DHCP PC C	57
Figura 17. Conexión mediante CMD a servidor web.....	58
Figura 18. Conexión mediante web a servidor web	59
Figura 19. Coincidencias recibidas por una lista de acceso	62
Figura 20. Restablecer los contadores de una lista de acceso	63
Figura 21. Restablecer los contadores de una lista de acceso	64
Figura 22. Con qué comando se muestran las traducciones NAT	65

GLOSARIO

CONECTIVIDAD: Se denomina a la conexión a una red de abonados puede ser por diferentes tipo como cableado o inalámbricos.

CONSOLA: Es una terminal que posee ciertos atributos para funciones específicas.

DNS: En español sistemas de nombre de dominio el cual realiza su función de convertir las direcciones lógicas numéricas a direcciones físicas como las páginas que podemos ver en nuestros pc.

DOMINIO: Permite esquematizar o segmentar grandes redes separadas de forma lógica donde pueden existir varios dominios.

INTERFAZ: Se denomina interfaz a la conexión física de los equipos que sirven para realizar conexiones a redes o demás host.

INTRANET: Es una red informática que permite la conectividad de servicios dentro de una organización.

IPCONFIG: Este comando es muy práctico en equipos Windows para saber su configuración de red.

IPV6: Debido a que en la actualidad se usa el tipo de direccionamiento ipv4 el cual tiene limitaciones de cantidad de host disponibles y debido al crecimiento de las redes por la cual se creó el protocolo de internet versión 6 la cual proporciona mayor cantidad de direcciones ip para los host de la red mundial.

NVRAM: Es la memoria física de algunos dispositivos electrónicos la cual permite que al tener fallas de tipo eléctrico el no pierda su configuración.

PING: Es una herramienta la cual nos permite en las redes de comunicaciones establecer desde un equipo terminal a equipos remotos si se tiene conexión determinando retardos o perdidas de paquetes.

QoS: Se define como el nivel de calidad de un servicio con respecto al cliente.

ROUTER: Es un equipo de red que permite encaminar varias redes de diferente segmento IP tomando la mejor ruta de origen a destino.

SSH: Es un protocolo que nos permite tener conexión entre equipos remotamente mediante un canal seguro previamente configurado.

SUBRED: Surge de la división de una red de gran tamaño debido a varios motivos ya sean reducir tamaño de dominios o mejorar su administración.

SWITCH: Es un equipo lógico de red el cual permite interconectar a varios terminales entre sí.

TERMINAL: Se pueden definir como cada uno de los ordenadores conectados a la red, también recibe el nombre de nodo o estación de trabajo.

TOPOLOGIA: Se puede considerar como la forma física de las redes de comunicaciones que pueden tomar varias ya definidas por diseño como estrella, mixta árbol entre otras.

TRACERROUTE: Este comando nos permite generar desde un equipo terminal a un equipo remoto generar la ruta mostrando la cantidad de saltos y tiempo de ejecución de la tarea.

UNIDIFUSION: Es una transmisión única para el tránsito de información a un receptor específico.

VTY: Las líneas vty nos permiten el acceso de equipos remotos a equipos cisco mediante telnet.

RESUMEN

El presente trabajo se realiza para mostrar las destrezas adquiridas del diplomado CCNA CISCO el cual fue tomado como opción de grado de la carrera de Ingeniería de Telecomunicaciones. En la prueba nos muestra dos escenarios propuestos los cuales requieren de aplicación básica de red como es direccionamiento ip enrutamiento y verificación de conectividad, para esto se realizara la simulación en el programa packet tracer que nos permite elaborarla y verificar el correcto funcionamiento con las herramientas de conexión con las que cuenta como ping traceroute entre otras.

Para el primer escenario nos solicita configurar aspectos básicos en swiches router y pc también diseñar la tabla de enrutamiento y generar administración de forma segura. En el segundo escenario nos solicitan montar conectividad mediante direccionamiento pv4 e ipv6, conexión OSPF, configuración dinámica de ip NAT,ACL y protocolos NTP.

Palabras Clave: Conectividad, Cisco, router, swith, networking

ABSTRACT

The present work is carried out to show the skills acquired from the CCNA CISCO diploma, which was taken as a degree option for the Telecommunications Engineering career. In the test it shows us two proposed scenarios which require a basic network application such as IP addressing, routing and connectivity verification, for this the simulation will be carried out in the package tracet program that allows us to elaborate it and verify the correct operation with the tools of connection with which it counts as ping traceroute among others.

For the first scenario, it asks us to configure basic aspects in router and PC switches, as well as design the routing table and generate administration in a secure way. In the second scenario, we are asked to set up connectivity through pv4 and ipv6 addressing, OSPF connection, dynamic configuration of ip NAT, ACL and NTP protocols.

Keywords: Connectivity, Cisco, router, swith, networking.

INTRODUCCIÓN

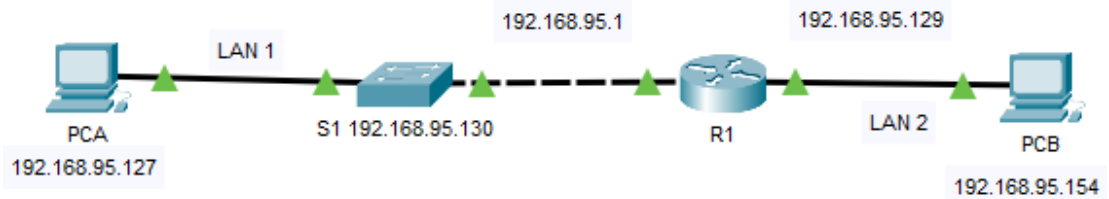
En el presente trabajo se realiza como opción de grado bajo la modalidad de proyecto aplicado en el cual se propone la realización de dos simulaciones con requerimientos específicos para la cual se requiere su elaboración en la herramienta de simulación packet tracer.

Como objetivos de desarrollo del escenario 1 se plantea construir la simulación de la red, realizar tabla de enrutamiento para redes y subredes, configurar equipos y dispositivos de red y finalmente verificar funcionamiento y conectividad en la red.

En el escenario 2 se propone implementación de una red OSPF y RIP con direccionamiento estático y dinámico con direccionamiento ip sin clase también se implementan paquetes de conmutación con protocolos STP y VLAN con dominios broadcast independientes, también se diseña un esquema de seguridad ip mediante protocolo DHCP mediante la traducción de ip sobre NAT-PAT respectivamente.

ESCENARIO 1

Figura 1: Topología escenario 1



Fuente propia

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el switch S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Parte 2: Desarrolle el esquema de direccionamiento IP

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

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla de direccionamiento

Tabla 1. Tabla de direccionamiento

Ítem	Requerimiento	Mascara
Dirección de Red	192.168.95.0	255.255.255.0/24
Requerimiento de host Subred LAN1	100	
Requerimiento de host Subred LAN2	50	
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.95.1	255.255.255.128/25
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.95.129	255.255.255.192/26
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.95.2	255.255.255.0 /25
PC-A	Ultima dirección de host de la subred LAN1 192.168.95.126	255.255.255.128/25
PC-B	Ultima dirección de host de la subred LAN2 192.168.95.190	255.255.255.192/26

Parte 3: Configure aspectos básicos R1 y S1

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Tabla Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	<pre>Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#exit Router# %SYS-5-CONFIG_I: Configured from console by console Router#</pre>
Nombre del router R1	<pre>Router#configure terminal Router(config)#hostname R1 R1(config)#exit</pre>
Nombre de dominio	<pre>R1#configure terminal R1(config)#ip domain-name ccna- lab.com R1(config)#exit R1#</pre>
Contraseña cifrada para el modo EXEC privilegiado	<pre>R1# R1#configure terminal R1(config)#enable secret ciscoenpass R1(config)#</pre>
Contraseña de acceso a la consola	<pre>R1# R1#configure terminal R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#exit R1#</pre>
Establecer la longitud mínima para las contraseñas	<pre>R1>enable Password: R1#configure terminal R1(config)#security password min- length 10 R1(config)#exit R1#</pre>
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	<pre>R1#configure terminal R1(config)#username admin secret admin1pass R1(config)#exit</pre>

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)# R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)# R1(config)#service password-encryption R1(config)#exit R1#
Configure un MOTD Banner	R1#configure terminal R1(config)#banner motd #Acceso denegado# R1(config)#exit R1#
Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1>enable Password: Password: R1#configure terminal R1(config)#interface gigabitEthernet 0/0/0 R1(config-if)#ip address 192.168.95.129 255.255.255.192 R1(config-if)#description esta la interfaz de la LAN 2 R1(config-if)#no shut R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up R1(config-if)#
Configurar interfaz G0/0/1 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1>enable User: Password: R1#configure terminal R1(config)#interface gi 0/0/1 R1(config-if)#ip address 192.168.95.1 255.255.255.128

	<pre> R1(config-if)#description esta la interfaz de la LAN 1 R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up </pre>
<p>Generar una clave de cifrado RSA Módulo de 1024 bits</p>	<pre> R1#configure terminal R1(config)#no ip domain-lookup R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com 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. How many bits in the modulus [512]: % Generating 512 bit RSA keys, keys will be non-exportable...[OK] R1(config)# *Mar 1 0:9:27.17: RSA key size needs to be at least 768 bits for ssh version 2 *Mar 1 0:9:27.17: %SSH-5-ENABLED: SSH 1.5 has been enabled R1# %SYS-5-CONFIG_I: Configured from console by console R1# </pre>

Las tareas de configuración para S1:

Tabla 3. Tabla Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup S1(config)#exit S1# S1#
Nombre del switch S1	Switch#configure terminal Router(config)#hostname S1 S1(config)#exit S1# S1#
Nombre de dominio ccna-lab.com	S1#configure terminal S1(config)#ip domain-name ccna-lab.com S1(config)#exit S1#
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	S1(config)#enable secret ciscoenpass S1(config)#line console 0
Contraseña de acceso a la consola ciscoconpass	S1(config)#line console 0 S1(config-line)#s
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1(config)#username admin password admin1pass S1(config)#exit S1#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#privilege level 4 S1(config-line)#transport input ssh

Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Acceso denegado# S1(config)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa general-keys modulus 1024 % You already have RSA keys defined named S1.ccna-lab.com % They will be replaced. % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non- exportable...[OK] *Mar 1 0:23:55.506: %SSH-5-ENABLED: SSH 1.99 has been enabled
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.95.2 255.255.255.128 S1(config-if)#no shutdown %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up %IP-4-DUPADDR: Duplicate address 192.168.58.1 on Vlan1, sourced by 0003.E4C5.E202 S1(config-if)#exit S1(config)#exit S1# %SYS S1(config)# S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.95.2 255.255.255.128 S1(config-if)#
Configuración del gateway predeterminado	S1(config-if)#

Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	S1(config-if)#ip default-gateway 192.168.95.1 S1(config)#exit S1# do wr
--	---

Paso 2. Configurar los equipos

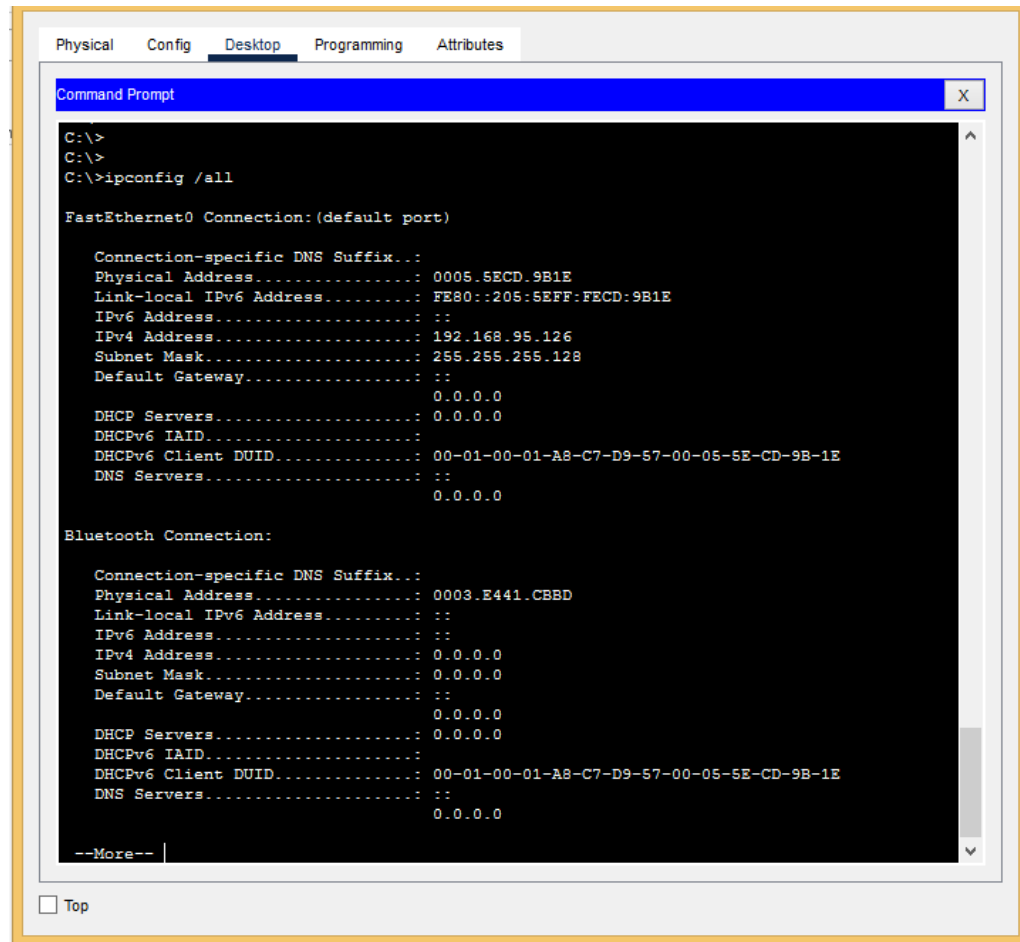
Configure los equipos host PC-A y PC-C conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

PC-A Network Configuration

Tabla 4. Configuración PC A

PC-A Network Configuration	
Descripción	PCA
Dirección física	0005.5ECD.9B1E
Dirección IP	192.168.95.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.95.1

Figura 2. Configuración PCA



Fuente propia

PC-C Network Configuración

Tabla 5. Configuración PC C

PC-B Network Configuración	
Descripción	PC C
Dirección física	0090.2112.01D9
Dirección IP	192.168.95.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.95.129

Figura 3. Configuración PC B

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address. . . . .: 0090.2112.01D9
Link-local IPv6 Address . . . . .: FE80::290:21FF:FE12:1D9
IPv6 Address. . . . .: ::
IPv4 Address. . . . .: 192.168.95.154
Subnet Mask . . . . .: 255.255.255.128
Default Gateway . . . . .: ::
                                0.0.0.0
DHCP Servers . . . . .: 0.0.0.0
DHCPv6 IAID . . . . .:
DHCPv6 Client DUID. . . . .: 00-01-00-01-02-D4-25-BD-00-90-21-12-01-D9
DNS Servers . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

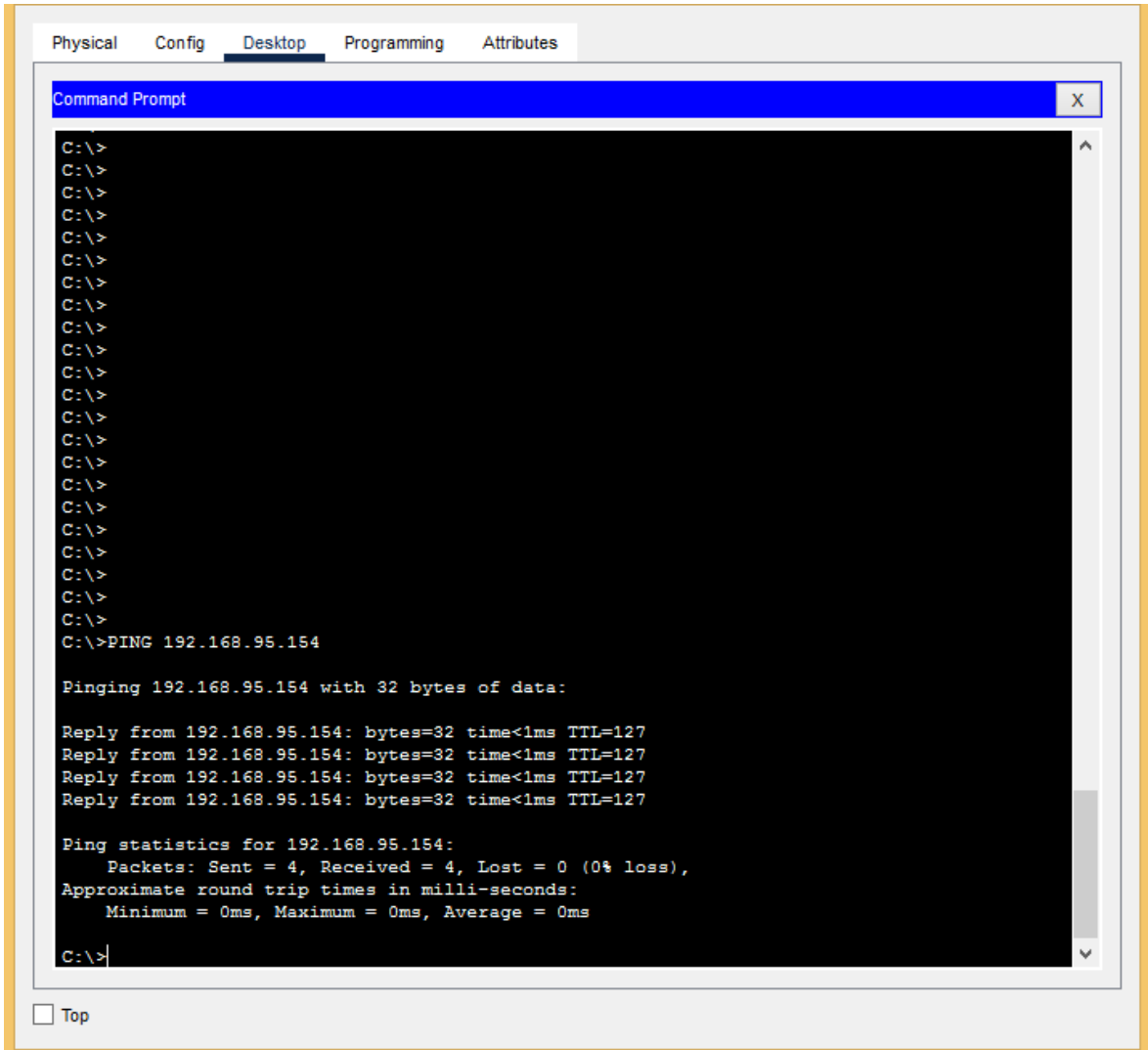
Connection-specific DNS Suffix...:
Physical Address. . . . .: 00D0.D337.25EE
Link-local IPv6 Address . . . . .: ::
IPv6 Address. . . . .: ::
IPv4 Address. . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: ::
                                0.0.0.0
DHCP Servers . . . . .: 0.0.0.0
--More--
```

Fuente propia

PRUEBA DE CONECTIVIDAD

PCA A CON DESTINO A PC B

Figura 4. Prueba de conectividad PC A.



The image shows a screenshot of a Command Prompt window titled "Command Prompt" with a blue header bar. The window is part of a larger application interface with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", where "Desktop" is selected. The Command Prompt displays a series of "C:\>" prompts. The 15th prompt is "C:\>PING 192.168.95.154". The output shows four successful replies from 192.168.95.154, each with 32 bytes of data, a time of less than 1ms, and a TTL of 127. Below the replies, the ping statistics are shown: "Ping statistics for 192.168.95.154: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms". The prompt "C:\>" is visible at the bottom of the window. A "Top" button is located at the bottom left of the window frame.

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>PING 192.168.95.154

Pinging 192.168.95.154 with 32 bytes of data:

Reply from 192.168.95.154: bytes=32 time<1ms TTL=127
Reply from 192.168.95.154: bytes=32 time<1ms TTL=127
Reply from 192.168.95.154: bytes=32 time<1ms TTL=127
Reply from 192.168.95.154: bytes=32 time<1ms TTL=127

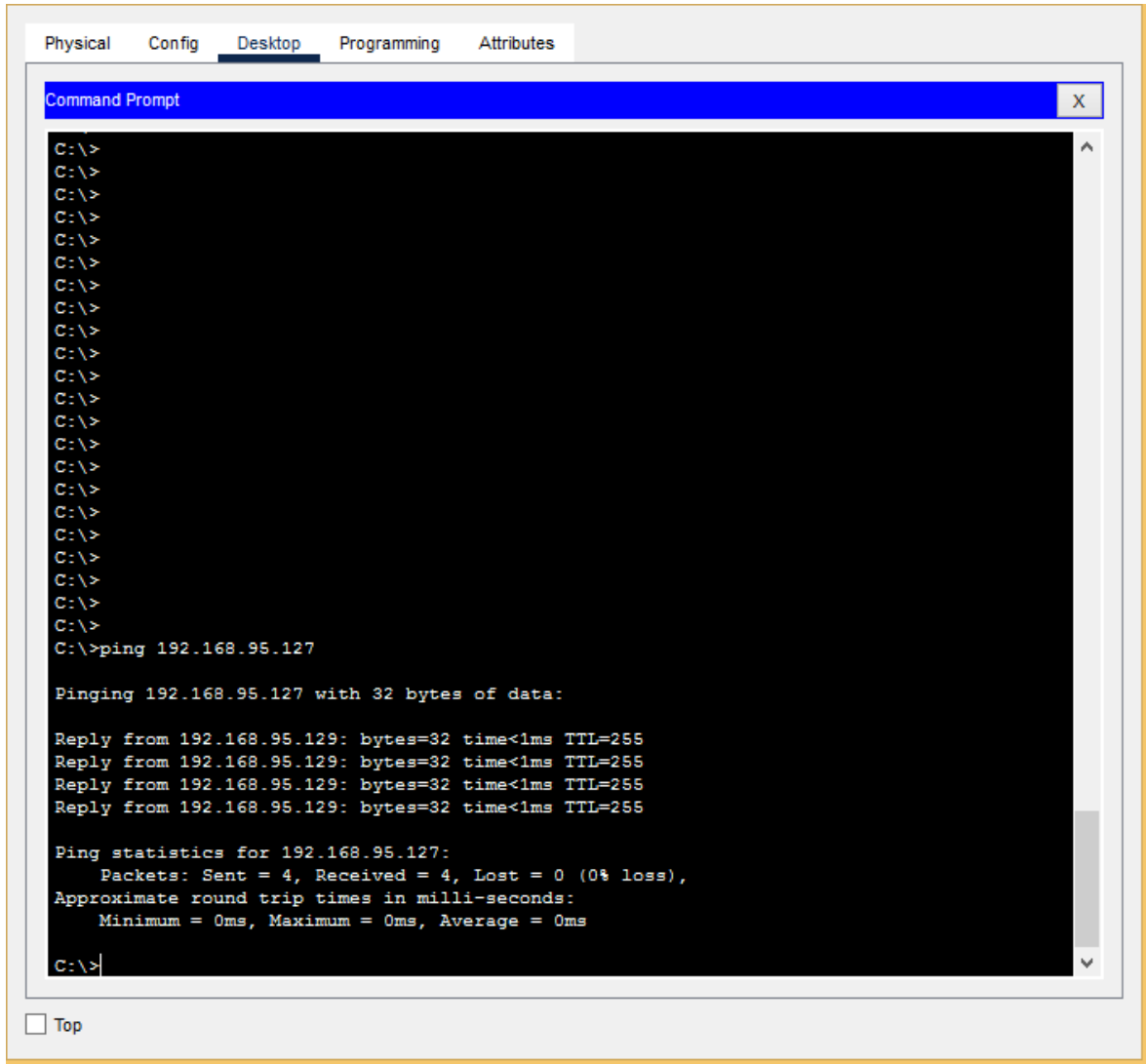
Ping statistics for 192.168.95.154:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente propia

PC C CON DESTINO A PC A

Figura 5. Prueba de conectividad PC B



The image shows a screenshot of a Command Prompt window within a software interface. The window title is "Command Prompt" and it has a blue title bar with a close button (X). The interface has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt shows the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.95.127

Pinging 192.168.95.127 with 32 bytes of data:

Reply from 192.168.95.129: bytes=32 time<1ms TTL=255
Reply from 192.168.95.129: bytes=32 time<1ms TTL=255
Reply from 192.168.95.129: bytes=32 time<1ms TTL=255
Reply from 192.168.95.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.95.127:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

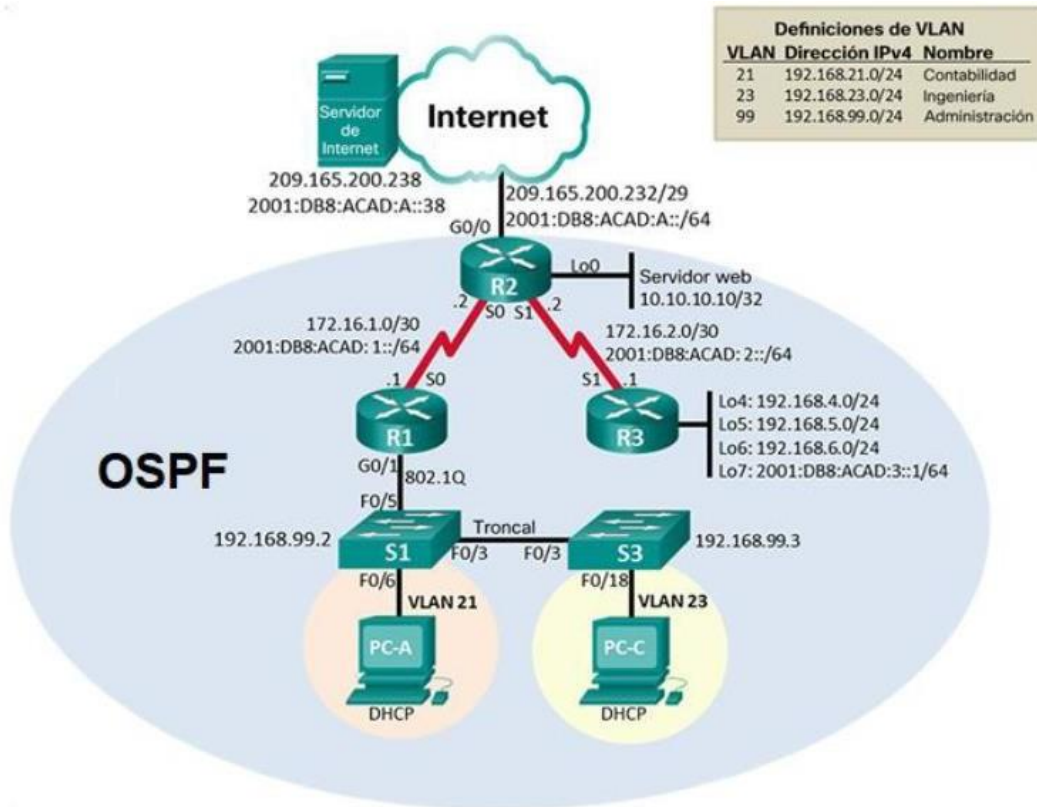
At the bottom of the window, there is a "Top" button with an unchecked checkbox.

Fuente propia

ESCENARIO 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 6. Topología de red escenario 2



Fuente guía diplomado.

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches. Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6. Iniciar dispositivos

Tarea	Comando de IOS
Elimina el archivo startup-config de todos los routers	Router>enable Router# erase startup-config
Volver a cargar todos los routers	Router#reload
Elimina el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch# erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload

Parte 2: Configurar los parámetros básicos de los dispositivos Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7. Parámetros básicos de los dispositivos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Paso 2: Configurar R1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R1	Router(config)#hostname R1
Contraseña de 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
Contraseña de acceso Telnet Cisco	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config)#service password- encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R1(config)#banner motd #Se prohíbe el acceso no autorizado #
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000	R1(config)# inter s0/2/0 R1(config-if)# description conection a server R1(config-if)#Ip address 209.165.200.238 255.255.255.248 Ipv6 address 2001:db8:acad:a::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut down

Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	<pre>R1(config)# inter s0/2/0 R1(config-if)# description conection a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shut down</pre> <p>Establece la descripción Establece la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establece la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establece la frecuencia de reloj en 128000 Activa la interfaz</p>
---	--

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R2	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada class	R2(config)#enable secret class
Contraseña de acceso a la consola Cisco	R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)# login
Contraseña de acceso Telnet Cisco	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login

Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server (este comando no lo permite el simulador)
Mensaje MOTD Se prohíbe el acceso no autorizado.	R2(config)#banner motd #Se prohíbe el acceso no autorizado #
Interfaz S0/2/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#int s0/2/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown Establece la descripción Establece la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establece la dirección IPv6. Según el diagrama de topología. Activa la interfaz
Interfaz S0/2/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de	R2(config-if)#int s0/2/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown Establece la descripción Establece la dirección IPv4. Se utiliza la primera dirección disponible en la subred. Establece la dirección IPv6. Usando el diagrama de topología para conocer la información de direcciones. Establece la frecuencia de reloj en 128000. Activa la interfaz

<p>direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz</p>	
<p>Interfaz G0/0/0 (simulación de Internet)</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>	<pre>R2(config-if)# int g0/0/0 R2(config-if)# description Connection to Internet R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)# no shutdown</pre>
<p>Interfaz loopback 0 (servidor web simulado)</p> <p>Establecer la descripción. Establezca la dirección IPv4.</p>	<pre>R2(config-if)#int loopback 0 R2(config-if)#%LINK-5-CHANGED: Interface Loopback0, changed state to up%LINEPROTO-5-UPDOWN: Line Interface Loopback0, changed state to up R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit</pre>

Ruta predeterminada	Se configura una ruta IPv4 predeterminada para G0/0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0
Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	Se configura una ruta IPv6 predeterminada para G0/0/0. R2(config)#ipv6 route ::/0 g0/0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada Class	R3(config)#enable secret class
Contraseña de acceso a la consola Cisco	R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)# login
Contraseña de acceso Telnet Cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R3(config)#banner motd #Se prohíbe el acceso no autorizado #

<p>Interfaz S0/0/1</p> <p>Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</p>	<pre>R3(config)#int s0/2/1 R3(config-if)#description conexion a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown</pre>
<p>Interfaz loopback 4</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p>	<pre>R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</pre> <p>Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.</p>
<p>Interfaz loopback 5</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p>	<pre>R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</pre> <p>Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.</p>
<p>Interfaz loopback 6</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p>	<pre>R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</pre> <p>Establece la dirección IPv4. Utiliza la primera dirección disponible en la subred.</p>
<p>Interfaz loopback 7</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p>	<pre>R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64</pre> <p>Establece la dirección IPv6. Usando el diagrama de topología para conocer la información de direcciones.</p>

Ruta predeterminada	Se configura una ruta IPv4 predeterminada para s0/2/1. R3(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0 Se configura una ruta IPv6 predeterminada para s0/2/1. R3(config)#ipv6 route ::/0 g0/0/0
---------------------	---

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada class	S1(config)#enable secret class
Contraseña de acceso a la consola cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet cisco	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S1(config)#banner motd #Se prohíbe el acceso no autorizado# S1(config)#exit

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada class	S3(config)#enable secret class
Contraseña de acceso a la consola cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	S3(config)#banner motd #Se prohíbe el acceso no autorizado# S3(config)#exit

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre 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 13. Verificación de conectividad mediante ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/2/0	2001:DB8:ACAD:1::2 172.16.1.2	Correcto
R2	R3, S0/2/0	2001:DB8:ACAD:2::1 172.16.2.2	Correcto
PC de Internet	Gateway predeterminado	2001:DB8:ACAD:A::1 209.165.200.238	Correcto

Figura 7. Desde R1 A R2

```

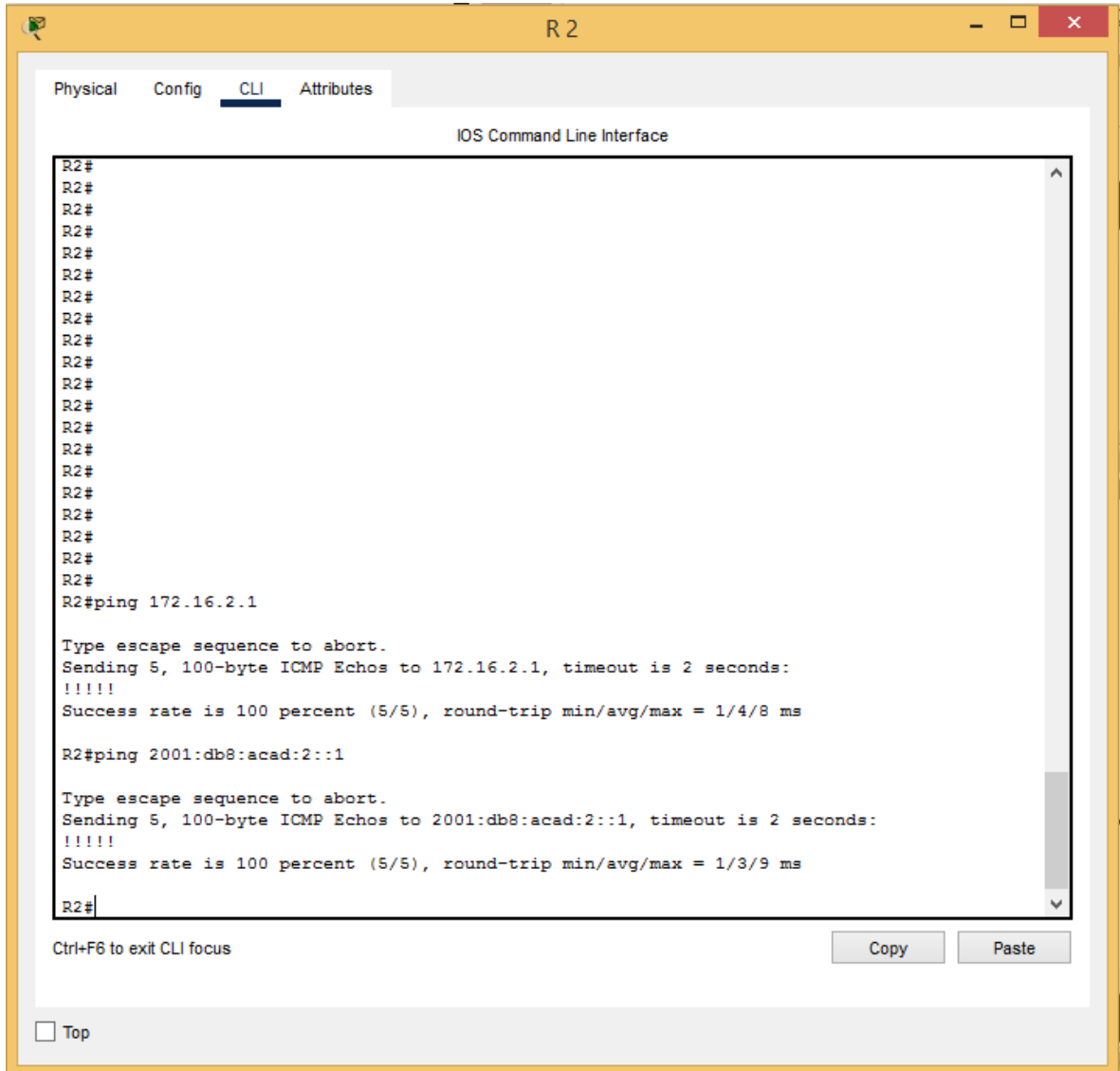
Router 1
Physical Config CLI Attributes
IOS Command Line Interface
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#ping 172.16.1.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.0, timeout is 2 seconds:

Reply to request 0 from 172.16.1.2, 6 ms
Reply to request 1 from 172.16.1.2, 1 ms
Reply to request 2 from 172.16.1.2, 1 ms
Reply to request 3 from 172.16.1.2, 7 ms
Reply to request 4 from 172.16.1.2, 7 ms

R1#ping 2001:db8:acad:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
R1#
    
```

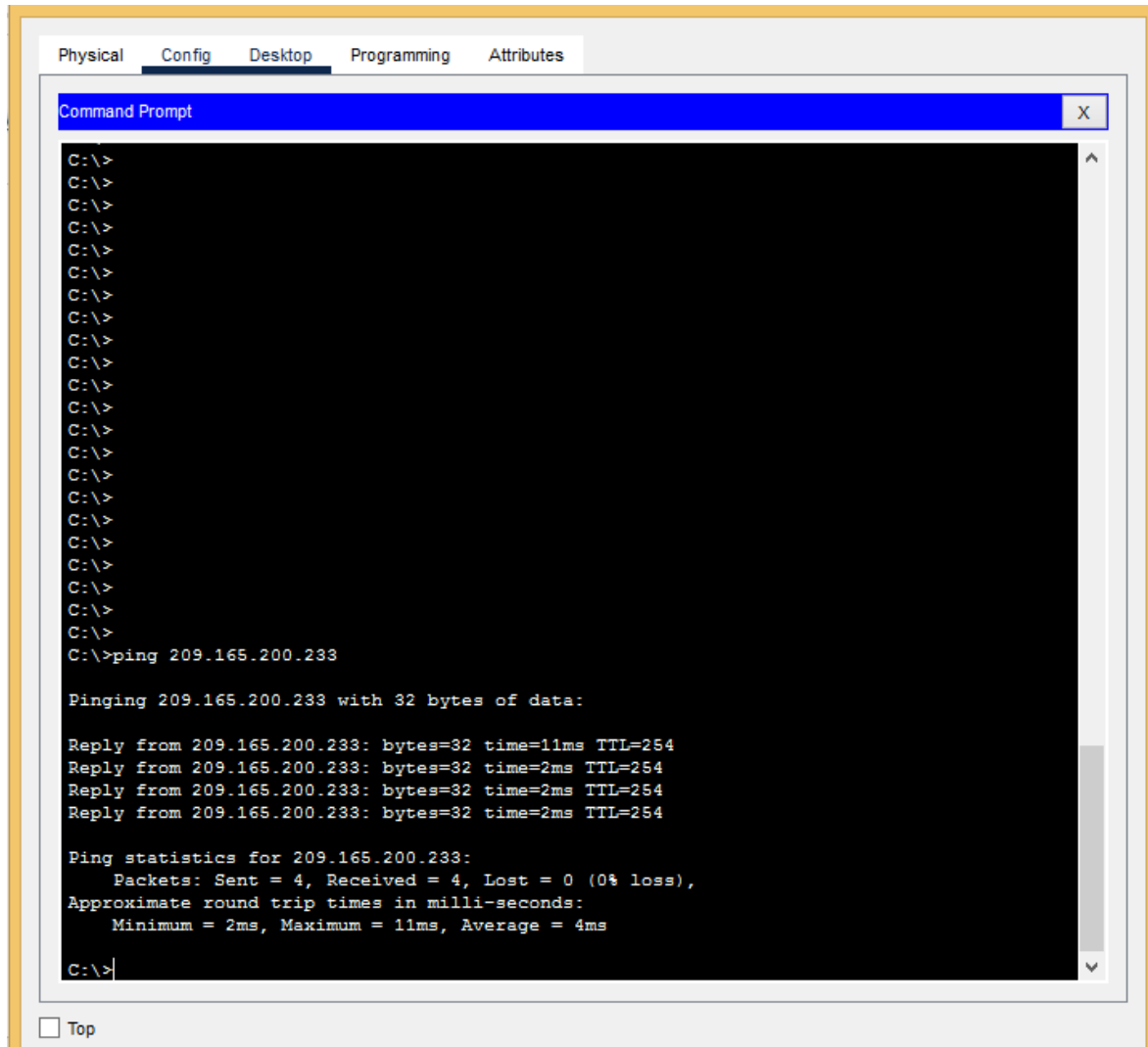
Fuente propia

Figura 8. Desde R2 A R3



Fuente propia

Figura 9 .Desde PC A Gateway



Fuente propia

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración de VLAN en S1

Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p> <p>Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican</p>	<p>S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name</p>
<p>Asignar la dirección IP de administración.</p> <p>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología</p>	<p>S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit</p>
<p>Asignar el gateway predeterminado</p> <p>Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.</p>	<p>S1(config)#ip default-gateway 192.168.99.1</p>
<p>Forzar el enlace troncal en la interfaz F0/3</p> <p>Utilizar la red VLAN 1 como VLAN nativa</p>	<p>S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</p>

Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1

Asignar la primera dirección IP en la subred como gateway predeterminado.	
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#int g0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0

<p>Configurar la subinterfaz 802.1Q .23 enG0/0/1</p> <p>Descripción: LAN de Ingeniería Asignar la VLAN 23</p> <p>Asignar la primera dirección disponible a esta interfaz</p>	<pre>R1(config)#int g0/0/1.23 R1(config-subif)#description LAN de Ing. R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0</pre>
<p>Configurar la subinterfaz 802.1Q .99 enG0/1</p> <p>Descripción: LAN de Administración Asignar la VLAN 99</p> <p>Asignar la primera dirección disponible a esta interfaz</p>	<pre>R1(config)#int g0/0/1.99 R1(config-subif)#description LAN de Admin R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0</pre>
<p>Activar la interfaz G0/1</p>	<pre>R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown</pre>

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

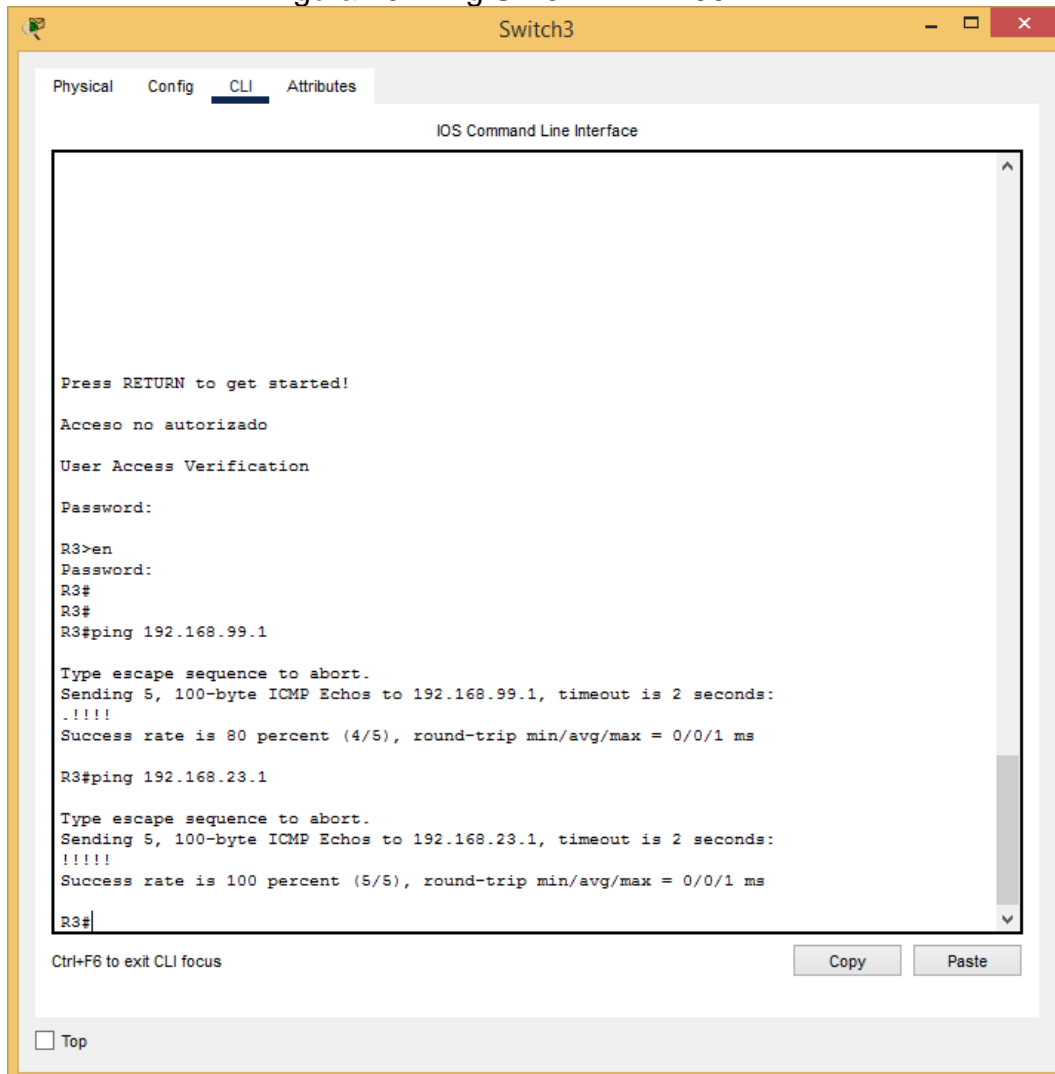
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Comprobación de conectividad

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Correcto
S3	R1, dirección VLAN 99	192.168.99.1	Correcto
S1	R1, dirección VLAN 21	192.168.21.1	Correcto

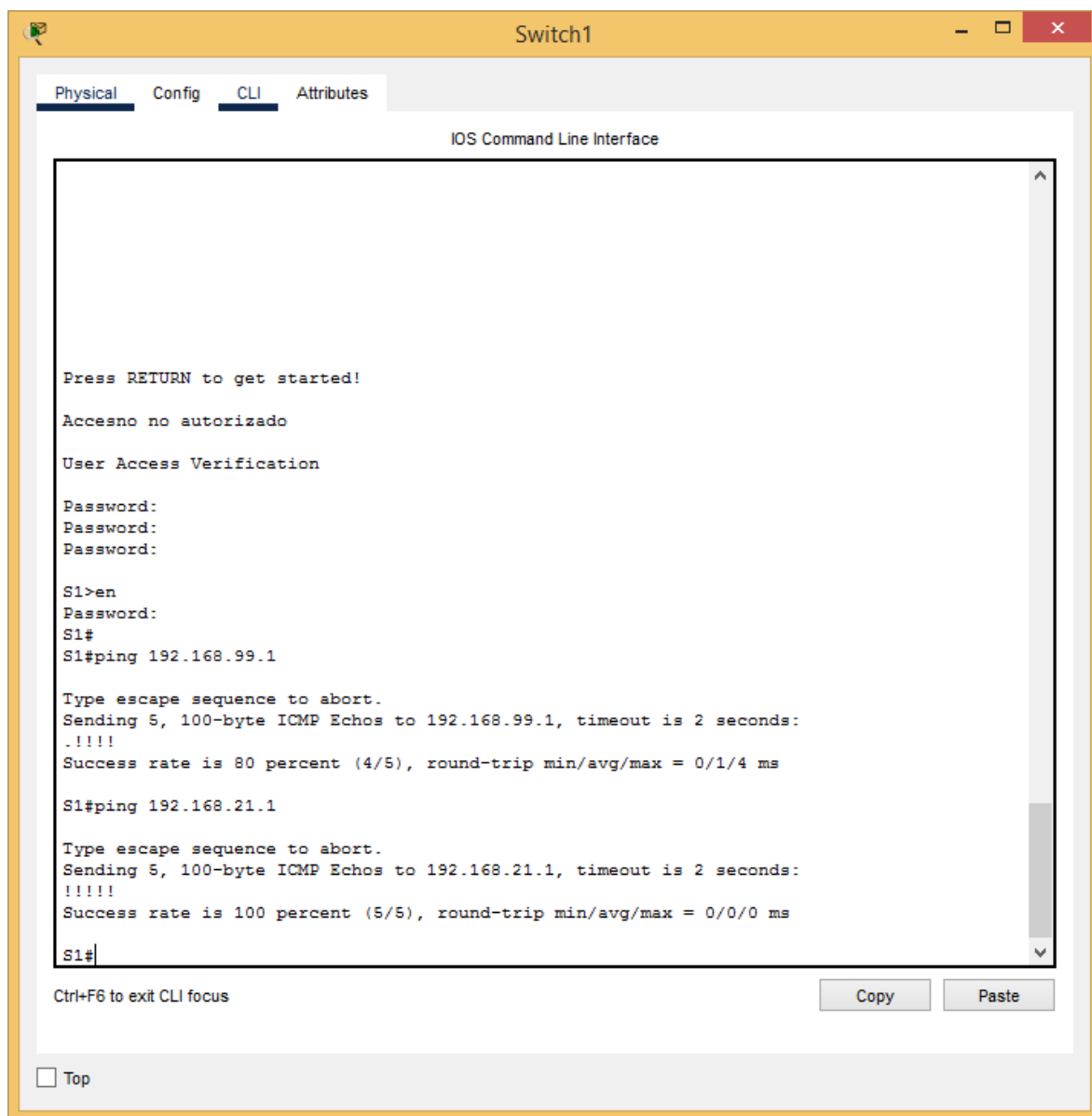
S3	R1, dirección VLAN 23	192.168.23.1	Correcto
----	-----------------------	--------------	----------

Figura 10. Ping SW3 A VLAN 99 Y 21.



Fuente propia

Figura 11.Ping SW32 A VLAN 99 Y 21.



Fuente propia

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18 .Configuración OSFP en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>enable R1#conf ter R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)# network 192.168.99.1 0.0.0.0 area 0 R1(config-router)# network 192.168.23.1 0.0.0.0 area 0 R1(config-router)# network 192.168.21.1 0.0.0.0 area 0 R1(config-router)# network 172.16.1.1 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interfac g0/0/1.21 R1(config-router)# passive-interfac g0/0/1.23 R1(config-router)# passive-interfac g0/0/1.99

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19.Configuración OSFP en R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2>enable R2#conf ter R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2

Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
	R2(config-router)#network 10.10.10. 0.0.0.0 area 0

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración OSPF V3 en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3>enable R3#conf ter R3(config)#router ospf 10 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.1 0.0.0.0 area 0 R3(config-router)#network 192.168.5.1 0.0.0.0 area 0 R3(config-router)#network 192.168.6.1 0.0.0.0 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive- interface loopback 4 R3(config-router)#passive- interface loopback 5 R3(config-router)#passive- interface loopback 6

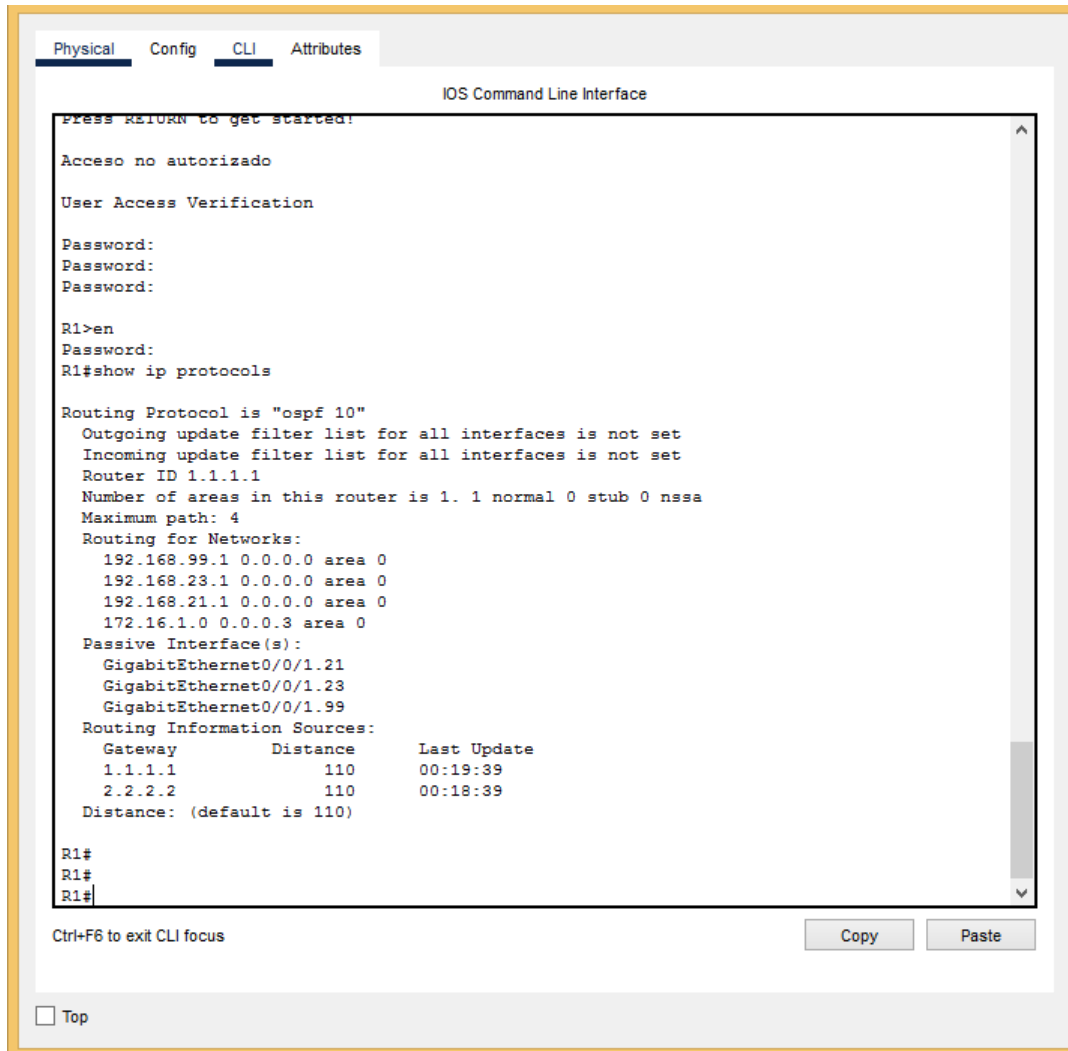
Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21.Verificacion OSFP

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Figura 12. Comprobación de configuración OSPF S1



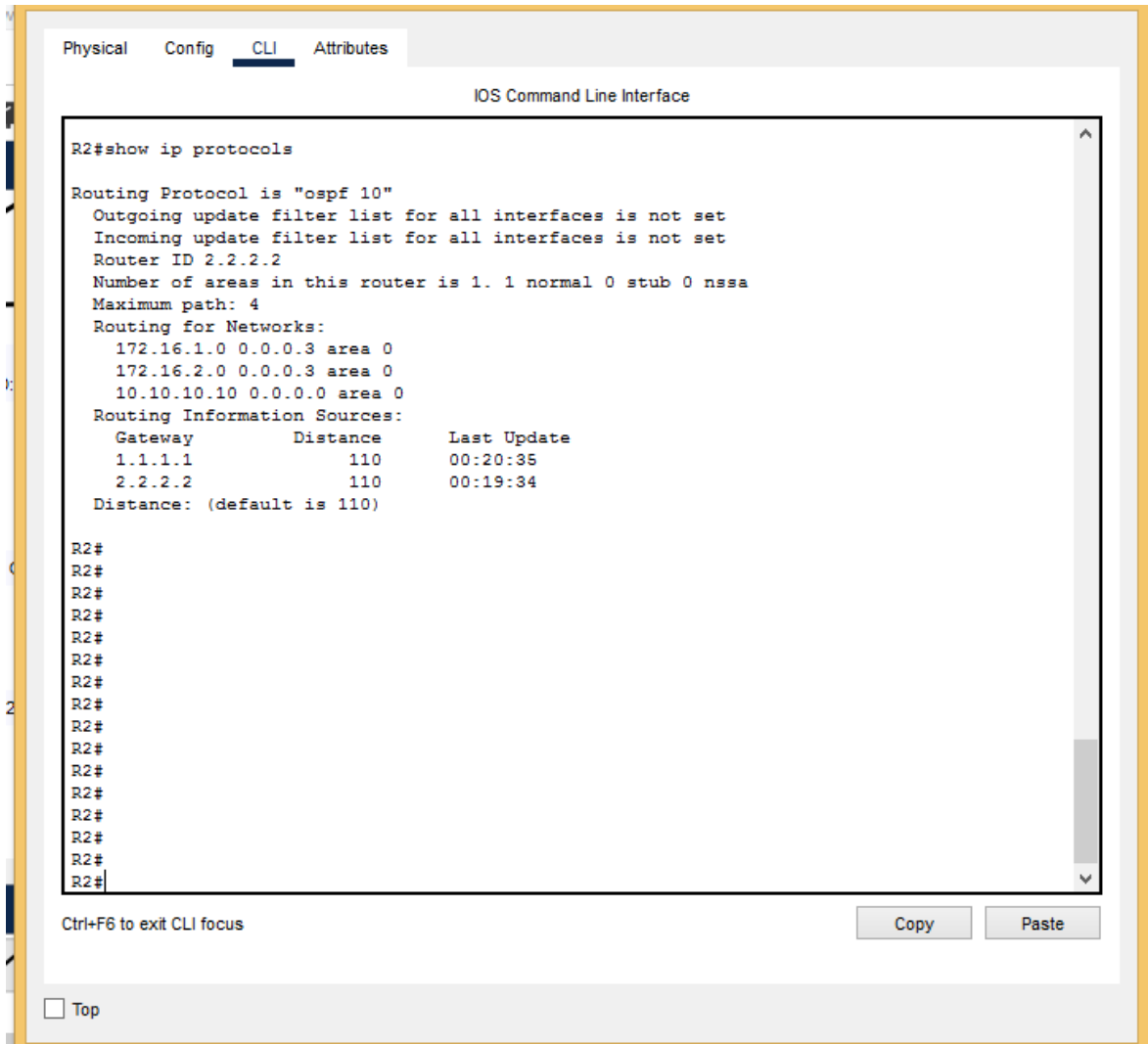
The screenshot displays the IOS Command Line Interface (CLI) for a router. The interface is titled "IOS Command Line Interface" and has tabs for "Physical", "Config", "CLI", and "Attributes". The CLI shows the following output:

```
Press RETURN to get started!  
Acceso no autorizado  
User Access Verification  
Password:  
Password:  
Password:  
R1>en  
Password:  
R1#show ip protocols  
Routing Protocol is "ospf 10"  
  Outgoing update filter list for all interfaces is not set  
  Incoming update filter list for all interfaces is not set  
  Router ID 1.1.1.1  
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
  Maximum path: 4  
  Routing for Networks:  
    192.168.99.1 0.0.0.0 area 0  
    192.168.23.1 0.0.0.0 area 0  
    192.168.21.1 0.0.0.0 area 0  
    172.16.1.0 0.0.0.3 area 0  
  Passive Interface(s):  
    GigabitEthernet0/0/1.21  
    GigabitEthernet0/0/1.23  
    GigabitEthernet0/0/1.99  
  Routing Information Sources:  
    Gateway         Distance      Last Update  
    1.1.1.1          110          00:19:39  
    2.2.2.2          110          00:18:39  
  Distance: (default is 110)  
R1#  
R1#  
R1#
```

At the bottom of the CLI window, there is a "Ctrl+F6 to exit CLI focus" message and two buttons: "Copy" and "Paste". A "Top" button is also visible at the bottom left of the window.

Fuente propia

Figura 13. Comprobación de configuración OSPF S2



The screenshot shows a network device's Command Line Interface (CLI) with the following output for the command 'show ip protocols':

```
R2#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    10.10.10.10 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:20:35
    2.2.2.2          110          00:19:34
  Distance: (default is 110)

R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
```

At the bottom of the CLI window, there is a 'Ctrl+F6 to exit CLI focus' message, 'Copy' and 'Paste' buttons, and a 'Top' button.

Fuente propia

Figura 14. Comprobación de configuración OSPF S3

```
Physical  Config  CLI  Attributes
IOS Command Line Interface

User Access Verification

Password:
Password:

R3>en
Password:
R3#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.16.2.0 0.0.0.3 area 0
    192.16.4.1 0.0.0.0 area 0
    192.168.4.1 0.0.0.0 area 0
    192.168.5.1 0.0.0.0 area 0
    192.168.6.1 0.0.0.0 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3          110          00:16:48
  Distance: (default is 110)

R3#
R3#
R3#
R3#
R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente propia

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración DHCP y VLAN en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>enable R1#conf ter R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21. Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23 Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye la siguiente tarea

Tabla 23. Configuración de NAT en R2

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p> <p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15</p>	<pre>R2>enable R2#conf ter R2(config)#username webuser privilege 15 secret cisco12345</pre>
<p>Habilitar el servicio del servidor HTTP</p>	<pre>R2(config)#ip http server Commando no reconocido</pre>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<pre>R2(config)#ip http authentication local Commando no reconocido</pre>
<p>Crear una NAT estática al servidor web.</p> <p>Dirección global interna: 209.165.200.229</p>	<pre>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229</pre>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<pre>R2(config)#int g0/0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/2/0 R2(config-if)#ip nat inside R2(config-if)#int s0/2/1 R2(config-if)#ip nat inside R2(config-if)#exit</pre>
<p>Configurar la NAT dinámica dentro de una ACL privada</p> <p>Lista de acceso: 1</p> <p>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1</p> <p>Permitir la traducción</p>	<pre>R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255</pre>

de un resumen de las redes LAN (loopback) en el R3	
<p>Defina el pool de direcciones IP públicas utilizables.</p> <p>Nombre del conjunto: INTERNET</p> <p>El conjunto de direcciones incluye:</p> <p>209.165.200.225 – 209.165.200.228</p>	<pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.0</pre> <p>Nombre del conjunto: INTERNET</p> <p>El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228</p>
Definir la traducción de NAT dinámica	<pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>

Paso 3: Verificar el protocolo DHCP y la NAT estática
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen

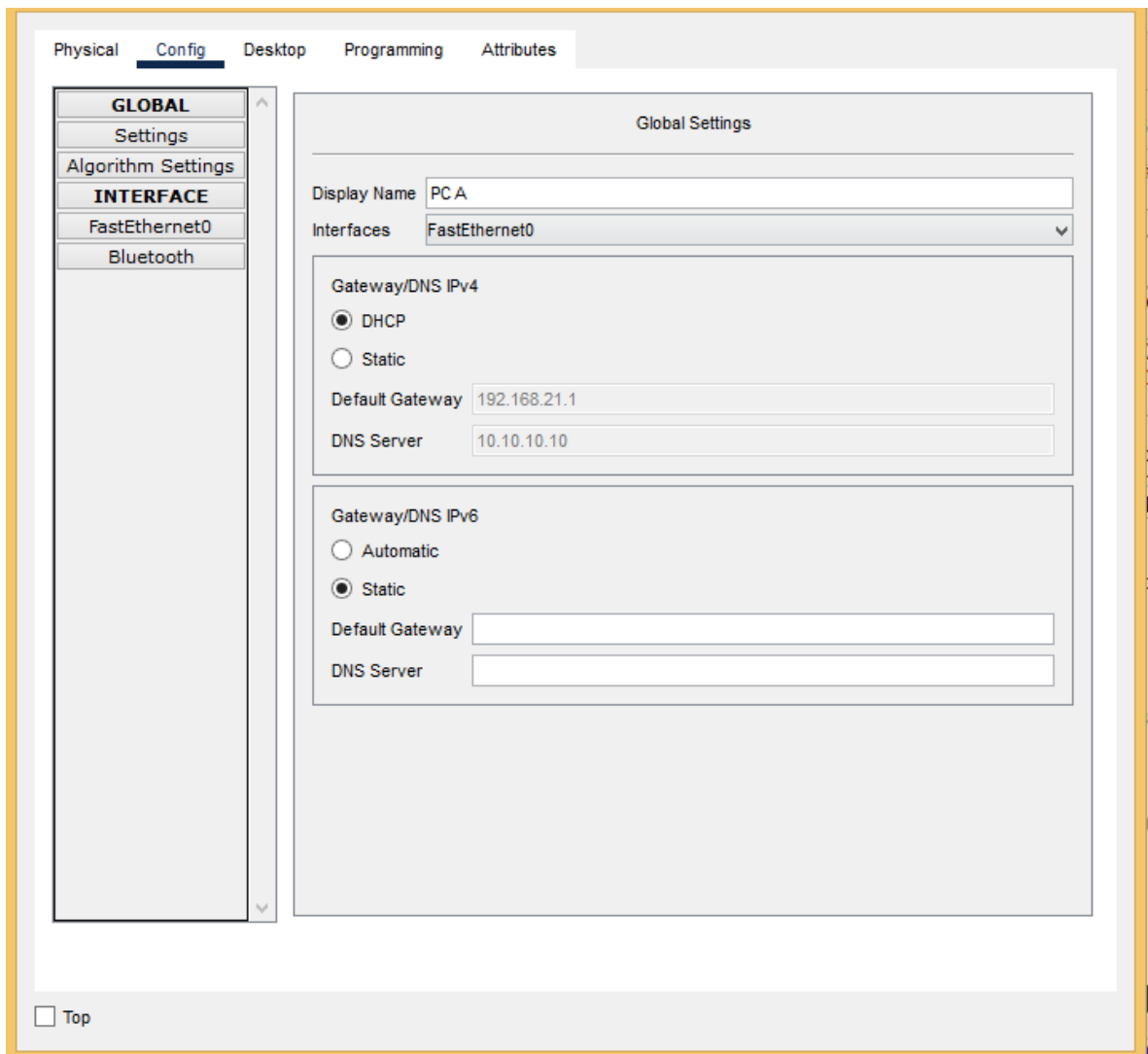
Tabla 24. Comprobación de conectividad DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Correcto
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Correcto
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Correcto

<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345</p>	<p>Correcto NOTA: Los comandos de habilitación hhttp en router 1 no fueron habilitados por este motivo se hace verificación mediante cmd PC C.</p>
--	---

COMPROBACION DE CONECTIVIDAD

Figura 15. Configuración DHCP PC A



Fuente propia

Figura 16. Configuración DHCP PC C

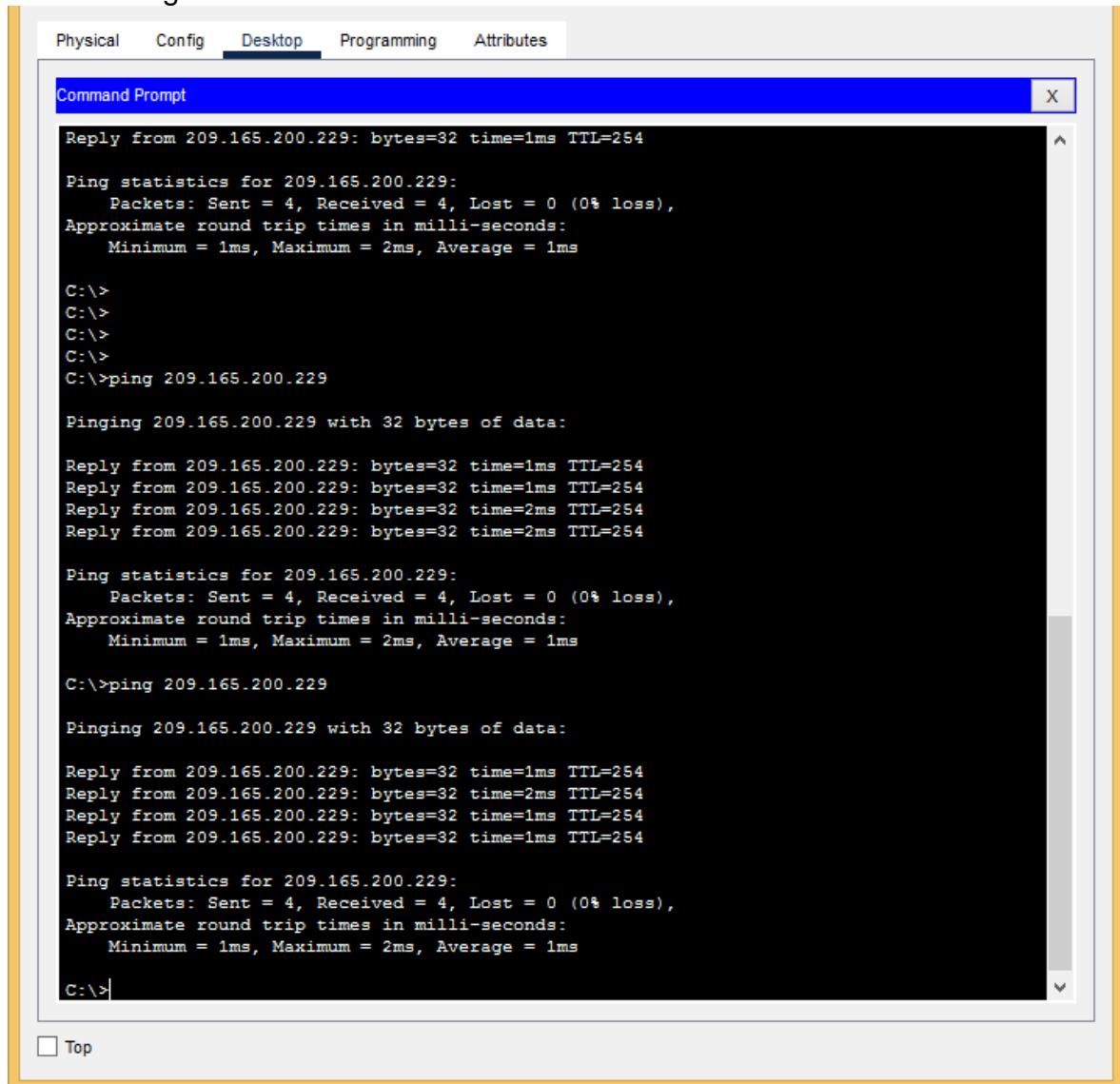
The image shows a network configuration interface with the following elements:

- Navigation tabs: Physical, **Config**, Desktop, Programming, Attributes.
- Left sidebar menu:
 - GLOBAL** (expanded)
 - Settings
 - Algorithm Settings
 - INTERFACE**
 - FastEthernet0
 - Bluetooth
- Main configuration area titled "Global Settings":
 - Display Name: PC B
 - Interfaces: FastEthernet0
 - Gateway/DNS IPv4:
 - DHCP
 - Static
 - Default Gateway: 192.168.23.1
 - DNS Server: 10.10.10.10
 - Gateway/DNS IPv6:
 - Automatic
 - Static
 - Default Gateway: [empty field]
 - DNS Server: [empty field]

Top

Fuente propia

Figura 17. Conexión desde PC C mediante CMD a servidor web.



The image shows a screenshot of a Windows Command Prompt window titled "Command Prompt". The window has a blue title bar and a black background with white text. The text displays the results of a ping command to the IP address 209.165.200.229. The output shows four successful replies with 32 bytes of data, 0% loss, and round trip times of 1ms and 2ms. The window also shows the current directory as C:\ and the prompt C:\>.

```
Physical Config Desktop Programming Attributes
Command Prompt X
Reply from 209.165.200.229: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
C:\>
C:\>
C:\>
C:\>ping 209.165.200.229

Pinging 209.165.200.229 with 32 bytes of data:

Reply from 209.165.200.229: bytes=32 time=1ms TTL=254
Reply from 209.165.200.229: bytes=32 time=1ms TTL=254
Reply from 209.165.200.229: bytes=32 time=2ms TTL=254
Reply from 209.165.200.229: bytes=32 time=2ms TTL=254

Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 209.165.200.229

Pinging 209.165.200.229 with 32 bytes of data:

Reply from 209.165.200.229: bytes=32 time=1ms TTL=254
Reply from 209.165.200.229: bytes=32 time=2ms TTL=254
Reply from 209.165.200.229: bytes=32 time=1ms TTL=254
Reply from 209.165.200.229: bytes=32 time=1ms TTL=254

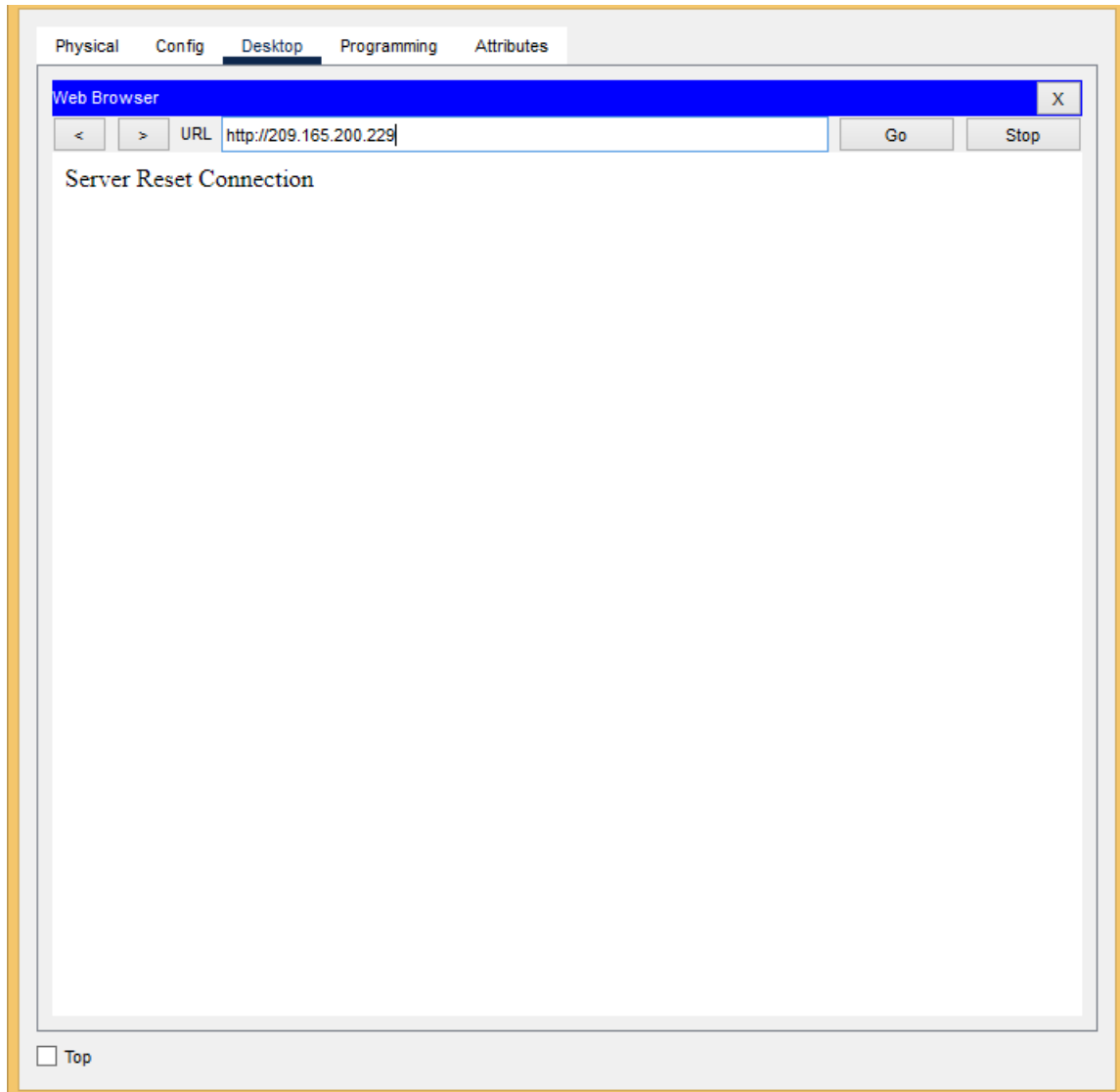
Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>|
```

Top

Fuente propia

Figura 18. Conexión mediante web DE PC C a servidor web.



Fuente propia

Parte 6: Configurar NTP

Tabla 25. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.	R2# clock set 9:00:00 5 March 2016 5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP. Nivel de estrato: 5	R2(config)#ntp master 5 Nivel de estrato: 5
Configurar R1 como un cliente NTP. Servidor: R2	R1(config)#ntp server 172.16.1.2 Servidor: R2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Configuración líneas VTY en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 Nombre de la ACL: ADMIN- MGT	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#transport input telnet
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

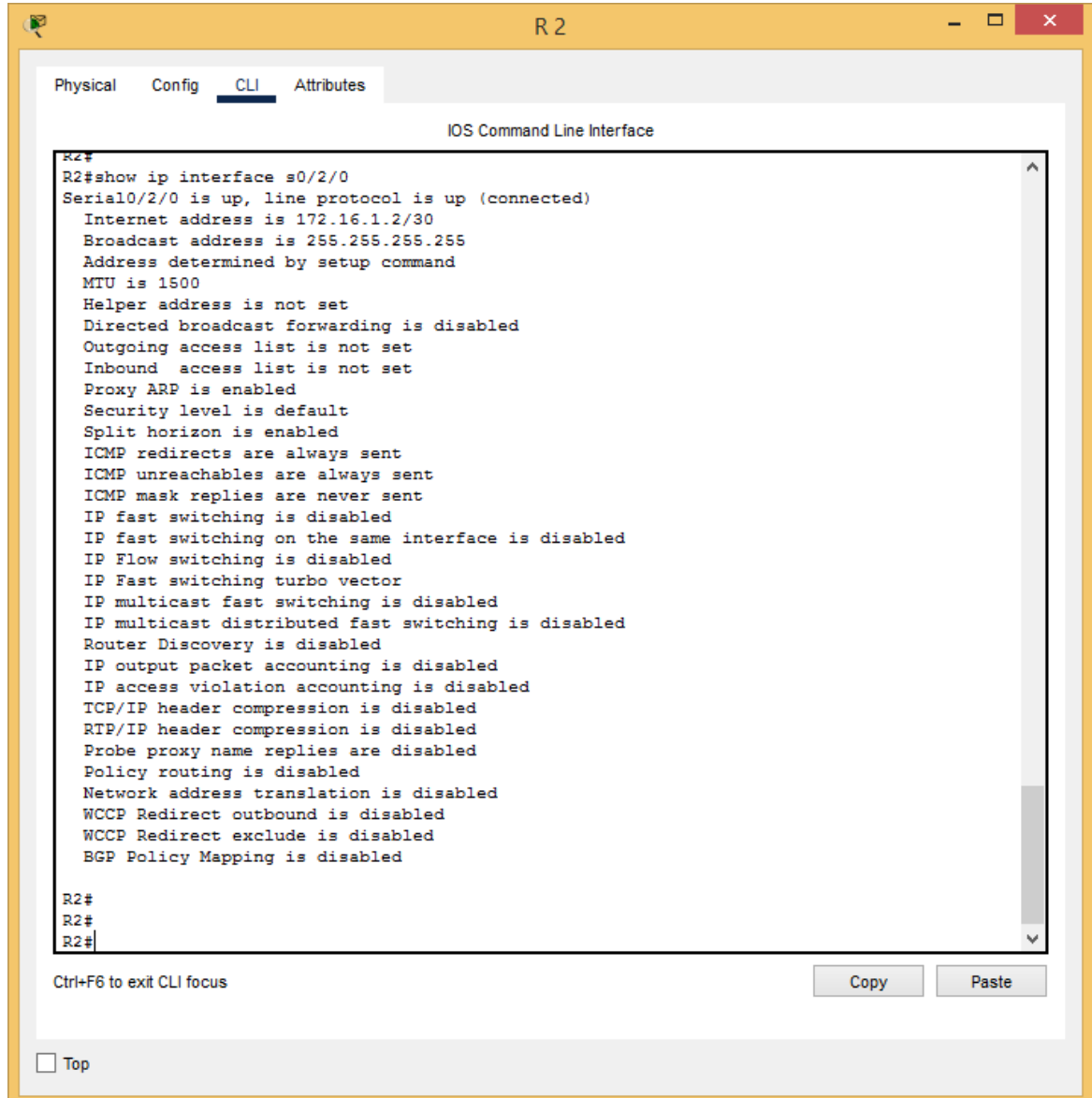
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2
--	----------------------

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. Verificación de configuración

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	R2#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección que se aplica?	R2#show ip interface s0/2/0
¿Con qué comando se muestran las traducciones NAT?	R2# show ip nat translations Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Figura 21. Restablecer los contadores de una listade acceso



Fuente propia

CONCLUSIONES

Se desarrolla el trabajo bajo modalidad de proyecto aplicado donde se da solución a los escenarios propuestos donde se analiza y se determinan los requerimientos específicos dando solución mediante herramientas de laboratorio simulado tiene gran variedad de herramientas para su aplicación. Se cumplió con el desarrollo del escenario uno donde se presentó la simulación de red esquema de direccionamiento, configuración de aspectos básicos de red y de seguridad en switch y router al igual que la verificación de conectividad de equipos.

Se logran los objetivos propuestos para el escenario dos, tales como: diseñar políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, para dar soluciones de red y conectividad escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN. Así mismo, configurar esquemas de conmutación de comunicación como NAT, PAT para la traducción de direcciones IP enrutamiento OSPF con el uso de direcciones en ambientes estáticos y mediante dhcp para comunicación entre VLAN y STP aplicados en la capa 2 de orden jerárquico convergente. Se brinda seguridad WAN.

En la aplicación y desarrollo de los escenarios propuestos se aplican conocimientos de routing y swiching escalabres en diferentes circunstancias y topologías al igual la empleabilidad en pequeñas organizaciones residenciales como en redes corporativas de gran escala esto genera mayor conceptualización de términos y aplicación a lo largo de la vida profesional.

BIBLIOGRAFÍA

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación, <https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#7>

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación, <https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#5>

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. <https://staticcourseassets.s3.amazonaws.com/RSE6/es/index.html#10>

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación, <https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#8>

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación, <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9>

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación, <https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#6>

CISCO. Principios básicos de routing y switching, <https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#7.1.1.1>

CISCO. Principios básicos de routing y switching, <https://contenthub.netacad.com/legacy/CCNA/RSE/6.0/es/index.html#6.1>