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

DEIBY LEANDRO ALVARADO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
BOGOTA D.C.
2020

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

DEIBY LEANDRO ALVARADO RODRÍGUEZ

Trabajo de Grado para obtener título en Ingeniería de Sistemas

Tutor
JOSE IGNACIO CARDONA
Ingeniero de Telecomunicaciones

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
BOGOTA D.C.
2020

Tabla de Contenido

Lista de Tablas....5
Lista de Figuras....7
Glosario....8
Resumen....10
ESCENARIO 1....11
Topología....11
Tabla de VLAN....11
Tabla de asignación de direcciones....11
PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS....12
Paso 1: Inicializar y volver a cargar el router y el Switch....12
Paso 2: Configurar R1....16
Paso 3: Configure S1 y S2....23
PARTE 2: CONFIGURACION DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)....29
Paso 4: Configurar S1....29
Paso 5: Configurar el S2....32
PARTE 3: CONFIGURAR SOPORTE DE HOSTS....35
Paso 6: Configure R1....35
Paso 7: Configurar los servidores....37
PARTE 4: PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO....39
ESCENARIO 2....42
Topología....42
PARTE 1: INICIALIZAR DISPOSITIVOS....42
Paso 1: Inicializar y volver a cargar los routers y los Switches....42
PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS....43
Paso 2: Configurar la computadora de Internet....43
Paso 3: Configurar R1....44
Paso 4: Configurar R2....48
Paso 5: Configurar R3....53
Paso 6: Configurar S1....58
Paso 6: Configurar S3....61
Paso 8: Verificar la conectividad de la red....64

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN 65
Paso 9: Configurar S1 65
Paso 10: Configurar S3 68
Paso 11: Configurar R1 71
Paso 12: Verificar la conectividad de la red 72
PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF 75
Paso 13: Configurar OSPF en el R1 75
Paso 14: Configurar OSPF en el R2 76
Paso 15: Configurar OSPFv3 en el R3 77
Paso 16: Verificar la información de OSPF 79
PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4 82
Paso 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 82
Paso 18: Configurar la NAT estática y dinámica en el R2 84
Paso 19: Verificar el protocolo DHCP y la NAT estática 86
PARTE 6: CONFIGURAR NTP 89
PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL) 92
Paso 20: Restringir el acceso a las líneas VTY en el R2 92
Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 95
Referencias Bibliográficas 101

Lista de Tablas

Tabla No. 1. Tabla de VLAN 11
Tabla No. 2. Asignación de direcciones 12
Tabla No. 3. Tareas configuración para R1 17
Tabla No. 4. Tareas configuración para S1 y S2 24
Tabla No. 5. Tareas configuración para S1 30
Tabla No. 6. Tareas configuración para S2 33
Tabla No. 7. Tareas configuración para R1 36
Tabla No. 8. Configuración de red PC-A. 38
Tabla No. 9. Configuración de red PC-B. 38
Tabla No. 10. Verificación conectividad de extremo a extremo 41
Tabla No. 11. Comandos IOS inicialización y cargue Routers y Switches. 43
Tabla No. 12. Configuración Servidor de Internet. 43
Tabla No. 13. Configuración para R1 45
Tabla No. 14. Configuración para R2 49
Tabla No. 15. Configuración para R3 54
Tabla No. 16. Configuración para S1 58
Tabla No. 17. Configuración para S3 61
Tabla No. 18. Verificación conectividad de la red 64
Tabla No. 19. Configuración del S1 66
Tabla No. 20. Configuración de S3 69
Tabla No. 21. Configuración de R1 71
Tabla No. 22. Verificación conectividad de la Red 74
Tabla No. 23. Configuración OSPF en el R1 75
Tabla No. 24. Configuración OSPF en el R2 76
Tabla No. 25. Configuración OSPF en el R3 78
Tabla No. 26. Verificación de la información de OSPF 79
Tabla No. 27. Configuración del R1 como servidor de DHCP para las VLAN 21 y 23 83
Tabla No. 28. Configuración NAT estática y dinámica en el R2 85
Tabla No. 29. Verificación del protocolo DHCP y la NAT estática 87

Tabla No. 30. Configuración NTP 89
Tabla No. 31. Restringir el acceso a las líneas VTY en el R2 92

Lista de Figuras

Figura No. 1. Topología de Red 11
Figura No. 2. Configuración equipo hosts PC-A. 38
Figura No. 3. Configuración equipo hosts PC-B. 39
Figura No. 4. Topología de Red Escenario 2 42
Figura No. 5. Configuración Servidor de Internet 44
Figura No. 6. Resultado Conectividad de R1 a R2, S0/1/0 65
Figura No. 7. Resultado Conectividad de R2 a R3, S0/1/1 65
Figura No. 8. Conectividad desde S1 a R1, dirección VLAN 99. 74
Figura No. 9. Conectividad desde S3 a R1, dirección VLAN 99. 74
Figura No. 10. Conectividad desde S1 a R1, dirección VLAN 21. 74
Figura No. 11. Conectividad desde S3 a R1, dirección VLAN 23. 74
Figura No. 12. Verificación comando Show ip protocols 80
Figura No. 13. Verificación comando Show ip route ospf. 81
Figura No. 14. Verificación comando Show ip ospf database 82
Figura No. 15. Verificación información PC-A – IP del servidor DHCP 88
Figura No. 16. Verificación información PC-C – IP del servidor DHCP 88
Figura No. 17. Verificación Conectividad PC-A al PC-C 89
Figura No. 18. Verificación Configuración de NTP en R1 92
Figura No. 19. Verificación de acceso Telnet desde R1 94
Figura No. 20. Verificación de acceso Telnet a R2 desde PC-A. 95
Figura No. 21. Verificación coincidencias recibidas por una lista de acceso desde la última vez que se restableció 97
Figura No. 22. Verificación qué ACL se aplica a una interfaz y la dirección en que se aplica 98
Figura No. 23. Verificación de las traducciones NAT 100

Glosario

Red:

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Internet:

Internet (el internet o, también, la internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyan una red lógica única de alcance mundial.

VLAN:

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

DHCP:

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

ISP:

El proveedor de servicios de Internet, (ISP, por las siglas en inglés de Internet Service Provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como ADSL, cable módem, GSM, dial-up, etc.

Router:

Un rúter,enrutador, (del inglés router) o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Switch:

Conmutador (Switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Resumen

El desarrollo del presente trabajo hace referencia a la solución de dos escenarios propuestos durante la ejecución de la actividad, donde se ponen a prueba los conocimientos adquiridos, realizando simulaciones mediante el aplicativo Packet Tracer, esto con el fin de desarrollar lo propuesto en la prueba de habilidades y solucionar los inconvenientes que surjan en el desarrollo del mismo.

Palabras Claves: Redes, Router, Switch, CISCO, direccionamiento.

Abstract

The development of this work refers to the solution of two scenarios proposed during the execution of the activity, where the acquired knowledge is tested, performing simulations using the Packet Tracer application, this in order to develop what is proposed in the test of skills and solve the inconveniences that arise in its development.

Keywords: Networks, Router, Switch, CISCO, addressing.

ESCENARIO 1

Topología

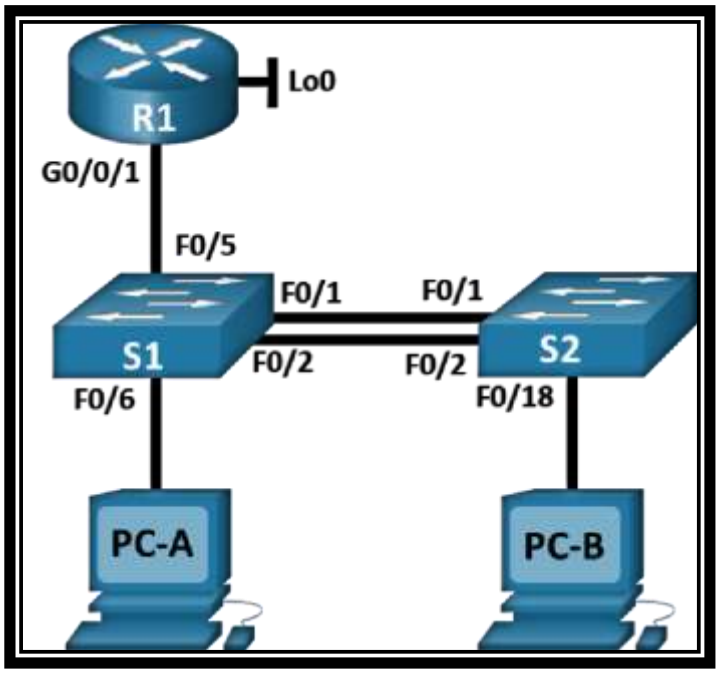

Figura No. 1. Topología de Red

En este primer 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. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla No. 1. Tabla de VLAN

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	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 dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Tabla No. 2. Asignación de direcciones

PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

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.

Se debe acceder a los dispositivos en modo privilegiado, donde vamos a ejecutar los comandos IOS y de este modo aceptaremos los mensajes de confirmación con el fin de inicializar los dispositivos.

a) Eliminación archivo de configuración del Router

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  Router> enable
  Router#

- Insertamos los comandos IOS para eliminar la configuración inicial, lo confirmamos con un Enter para su ejecución.

  Router# erase startup-config
  Erasing the nvram filesystem will remove all configuration files!
  Continue? [confirm]
  [OK]
  Erase of nvram: complete
  %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
  Router#

- Procedemos a realizar el cargue del dispositivo y aceptamos la confirmación.

  Router#reload
  Proceed with reload? [confirm]

  Nos saldrá un mensaje que si deseamos acceder al dialogo de configuración inicial, le damos que “no”

  Would you like to enter the initial configuration dialog? [yes/no]: no

b) Eliminación archivo de configuración del Switch

- Se determina si se crearon redes de área local virtuales

  Switch# show flash

- Si llegase a existir algún archivo VLAN se procedería a realizar la eliminación, luego de ejecutar el comando se debe hacer la confirmación.

Switch# delete vlan.dat
Delete filename [vlan.dat]?

- Insertamos los comandos IOS para eliminar la configuración inicial, lo confirmamos con un Enter para su ejecución.

  Switch# erase startup-config
  Erasing the nvram filesystem will remove all configuration files!
  Continue? [confirm]
  [OK]
  Erase of nvram: complete
  %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
  Switch#

- Procedemos a realizar el cargue del dispositivo y aceptamos la confirmación.

  Switch# reload
  Proceed with reload? [confirm]

- Después de recargar el Switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el Switch.

  a) Configuración de la plantilla SDM para que admita IPV6 en el Switch.

  - Lo que hacemos es verificar las plantillas que se encuentran predeterminadas en el Switch.

    La plantilla actual del Switch es “desktop default”. Esta plantilla lo que hace es optimizar los recursos.

    Switch# show sdm prefer
    The current template is "desktop default" template.
    The selected template optimizes the resources in
    the switch to support this level of features for
    8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:	6K
number of IPv4 IGMP groups + multicast routes:	1K
number of IPv4 unicast routes:	8K
number of directly-connected IPv4 hosts:	6K
number of indirect IPv4 routes:	2K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	1K

De acuerdo a esto podemos evidenciar que la plantilla predeterminada es compatible con 8 interfaces enrutadas, pero no se evidencia en ningún momento una característica IPV6 habilitada, por lo tanto toca realizar el proceso adecuado para habilitarla.

- Procedemos a ingresar a la configuración del Switch.

  Switch# config t
  Enter configuration commands, one per line. End with CNTL/Z.
  Switch(config)#

- Procedemos a seleccionar la plantilla dual-ipv4-and-ipv6, teniendo en cuenta que es la plantilla que nos interesa, pero antes debemos revisar que opciones nos ofrece la plantilla, por lo que digitamos:

  Switch(config)#sdm prefer dual-ipv4-and-ipv6 ?
  default Default bias
  routing Unicast bias
  vlan Vlan bias
  Switch(config)#

- Podemos observar las opciones que tiene la plantilla, lo que nos da a entender que podemos otorgar recursos al enrutamiento IPV4 e IPV6, o podemos otorgar recursos a VLAN, de acuerdo a esto seleccionare las opciones predeterminadas (default).

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

- De acuerdo al mensaje emitido, las preferencias seleccionadas de la plantilla SDM, tendrán efecto tan pronto realice la recarga de Switch, por lo tanto procedo a realizar la recarga.

  Tan pronto se realice la recarga nos emitirá un mensaje que dice que la configuración del sistema fue modificada, que si deseamos guardarla, para lo que respondemos que SI.

  Switch#reload
  System configuration has been modified. Save? [yes/no]:yes

Building configuration...
[OK]
Proceed with reload? [confirm]

- Tan pronto se inicie nuevamente el Switch, lo que hacemos es verificar si ya quedo habilitado el protocolo IPV6.

Switch>enable
Switch#show sdm prefer
The current template is "desktop IPv4 and IPv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:	2K
number of IPv4 IGMP groups + multicast routes:	1K
number of IPv4 unicast routes:	3K
number of directly-connected IPv4 hosts:	2K
number of indirect IPv4 routes:	1K
number of IPv6 multicast groups:	1.125k
number of directly-connected IPv6 addresses:	2K
number of indirect IPv6 unicast routes:	1K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	1K
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.625k
number of IPv6 security aces:	0.5K

Switch#

- Este procedimiento debe ser realizado en ambos Switches, teniendo en cuenta que ambos se deben configurar con protocolo IPV4 e IPV6.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1

Tarea	Especificación
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar VTY solo aceptando SSH	
Cifrar las contraseñas de texto no cifrado	
Configure un MOTD Banner	
Habilitar el routing IPv6	
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Tabla No. 3. Tareas configuración para R1.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

Router> enable
Router#

- Procedemos a ingresar al modo de configuración.

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

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

  Router(config)#no ip domain-lookup
  Router(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

  Router#show run | include domain-lookup
  no ip domain-lookup
  Router#

- Procedemos a guardar la configuración NVRAM.

  Router#copy run start
  Destination filename [startup-config]?
  Building configuration...
  [OK]
  Router#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Router mediante el comando “hostname R1”, damos Enter y salimos del modo de configuración.

  Router(config)#hostname R1
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console
  R1#

c) Nombre de dominio

- Procedemos a habilitar la resolución de nombres en el Router

  R1(config)#ip domain-lookup
  R1(config)#

- Procedemos a definir el nombre del Dominio

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

- Procedemos a desactivar nuevamente la resolución DNS en el Router y salimos del modo de configuración.

  R1(config)#no ip domain-lookup
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console
  R1#

d) Contraseña cifrada para el modo EXEC privilegiado

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

  R1(config)#enable secret ciscoenpass
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console
  R1#

e) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

  R1(config)#line console 0
  R1(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

  R1(config-line)#password ciscoconpass
  R1(config-line)#login
  R1(config-line)#exit
  R1(config)#exit

R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

f) Establecer la longitud mínima para las contraseñas

- Procedemos a establecer la longitud mínima para las contraseñas y salimos del modo de configuración.

R1(config)#security passwords min-length 10
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

g) Crear un usuario administrativo en la base de datos local

- Lo que hacemos ahora es definir la configuración global del Usuario y la Contraseña

R1(config)#username admin password admin1pass
R1(config)#

- Ahora, procedemos a indicarle al router que autentique con el usuario y contraseña.

R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#

- Con esta configuración lo que hacemos es indicarle al router que ya no haga caso al password configurado de consola, si no que busque la base de datos local para el usuario y la contraseña.

User Access Verification

Username: admin
Password:

R1>

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

- Ahora, procedemos a indicarle al Router que en las líneas VTY solicite el usuario y contraseña local.

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

i) Configurar VTY solo aceptando SSH

- Ahora, procedemos a editar los puertos VTY para que solo permita el acceso por SSH.

  R1(config)#line vty 0 15
  R1(config-line)#transport input ssh
  R1(config-line)#login local

j) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

  R1(config)#service password-encryption
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console
  R1#

k) Configure un MOTD Banner

- Procedemos a ingresar el mensaje de acceso al Router

  R1(config)#banner motd "Acceso Restringido, Solo el personal administrador puede acceder"
  R1(config)#

l) Habilitar el routing IPv6

- Procedemos a realizar la activación del protocolo IPV6 a nivel global.

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

m) Configurar interfaz G0/1 y subinterfaces

- Procedemos a ingresar a la interfaz GigabitEthernet0/1.2, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para R1 y la tabla de asignación de direcciones.

  R1(config)#interface g0/1.2
  R1(config-subif)#encapsulation dot1Q 2
  R1(config-subif)#description Bikes
  R1(config-subif)#ip address 10.19.8.1 255.255.255.192
  R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
  R1(config-subif)#ipv6 addres fe80::1 link-local
  R1(config-subif)#

- Procedemos a ingresar a la interfaz GigabitEthernet0/1.3, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para R1 y la tabla de asignación de direcciones.

  R1(config)#interface g0/1.3
  R1(config-subif)#encapsulation dot1Q 3
  R1(config-subif)#description Trikes
  R1(config-subif)#ip address 10.19.8.65 255.255.255.224
  R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
  R1(config-subif)#ipv6 address fe80::1 link-local
  R1(config-subif)#

- Procedemos a ingresar a la interfaz GigabitEthernet0/1.4, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para R1 y la tabla de asignación de direcciones.

  R1(config)#interface g0/1.4
  R1(config-subif)#encapsulation dot1Q 4
  R1(config-subif)#description Management
  R1(config-subif)#ip address 10.19.8.97 255.255.255.248
  R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
  R1(config-subif)#ipv6 address fe80::1 link-local
  R1(config-subif)#

- Procedemos a ingresar a la interfaz GigabitEthernet0/1.6, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para R1 y la tabla de asignación de direcciones.

  R1(config)#interface g0/1.6
  R1(config-subif)#encapsulation dot1Q 6
  R1(config-subif)#description Native

- Ahora procedemos a habilitar la interfaz.

R1(config)#interface g0/1
R1(config-if)#no shutdown

n) Configure el Loopback0 interface

- Procedemos a ingresar a la interfaz Loopback0, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para R1 y la tabla de asignación de direcciones.

R1(config-if)#interface Loopback 0
R1(config-if)#description Loopback
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)#exit
R1(config)#

o) Generar una clave de cifrado RSA

- Ahora procedemos a establecer la clave de cifrado

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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1 o S2, según proceda**

Tarea	Especificación
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Tabla No. 4. Tareas configuración para S1 y S2.

La configuración y desarrollo de los presentes puntos fueron establecidos en los Switches S1 y S2.

a) Desactivar la búsqueda DNS.

- Se accede al Switch, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

Switch>enable
Switch#

- Procedemos a ingresar al modo de configuración.

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

  Switch(config)#no ip domain-lookup
  Switch(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

  Switch#show run | include domain-lookup
  no ip domain-lookup
  Switch#

- Procedemos a guardar la configuración NVRAM.

  Switch#copy run start
  Destination filename [startup-config]?
  Building configuration...
  [OK]
  Switch#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Switch mediante el comando “hostname S1”, damos Enter y salimos del modo de configuración.

  Switch(config)#hostname S1
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

c) Nombre de dominio

- Procedemos a habilitar la resolución de nombres en el Router

  S1(config)#ip domain-lookup
  S1(config)#

- Procedemos a definir el nombre del Dominio

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

- Procedemos a desactivar nuevamente la resolución DNS en el Router y salimos del modo de configuración.

  S1(config)#no ip domain-lookup
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

d) Contraseña cifrada para el modo EXEC privilegiado

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

  S1(config)#enable secret ciscoenpass
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

e) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

  S1(config)#line console 0
  S1(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

  S1(config-line)#password ciscoconpass
  S1(config-line)#login
  S1(config-line)#exit
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

f) Crear un usuario administrativo en la base de datos local

- Lo que hacemos ahora es definir la configuración global del Usuario y la Contraseña

  S1(config)#username admin password admin1pass
  S1(config)#

- Ahora, procedemos a indicarle al router que autentique con el usuario y contraseña.

  S1(config)#line console 0
  S1(config-line)#login local
  S1(config-line)#

- Con esta configuración lo que hacemos es indicarle al router que ya no haga caso al password configurado de consola, si no que busque la base de datos local para el usuario y la contraseña.

  User Access Verification

  Username: admin
  Password:

  S1>

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

- Ahora, procedemos a indicarle al Switch que en las líneas VTY solicite el usuario y contraseña local.

  S1(config)#line vty 0 15
  S1(config-line)#login local
  S1(config-line)#exit
  S1(config)#

h) Configurar VTY solo aceptando SSH

- Ahora, procedemos a editar los puertos VTY para que solo permita el acceso por SSH.

  S1(config)#line vty 0 15
  S1(config-line)#transport input ssh
  S1(config-line)#login local

i) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#

j) Configure un MOTD Banner

- Procedemos a ingresar el mensaje de acceso al Router

S1(config)#banner motd "Acceso Restringido, Solo el personal administrador puede acceder"
S1(config)#

k) Generar una clave de cifrado RSA

- Ahora procedemos a establecer la clave de cifrado

S1(config)#crypto key generate rsa
The name for the keys will be: S1.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S1(config)#

l) Configurar la interfaz de administración (SVI)

- Procedemos a ingresar a la interfaz vlan 4, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para S1 y la tabla de asignación de direcciones.

S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64

S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#

- Procedemos a ingresar a la interfaz vlan 4, para realizar las respectivas configuraciones de acuerdo a la tabla de configuración para S2 y la tabla de asignación de direcciones.

S2(config)#interface vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#

m) Configuración del Gateway predeterminado

- Procedemos a configurar la puerta de enlace predeterminada para el protocolo IPV4.

S1(config)#ip default-gateway 10.19.8.97
S1(config)#

PARTE 2: CONFIGURACION DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla No. 5. Tareas configuración para S1.

a) Crear VLAN

- Se accede al Switch, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  User Access Verification

  Username: admin
  Password:
  S1>enable
  Password:
  S1#

- Procedemos a ingresar al modo de configuración.

  S1#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  S1(config)#

- Ahora procedemos a crear las VLAN

  S1(config)#vlan 2
  S1(config-vlan)#name Bikes
  S1(config-vlan)#vlan 3
  S1(config-vlan)#name Trikes
  S1(config-vlan)#vlan 4
  S1(config-vlan)#name Management
  S1(config-vlan)#vlan 5

S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native

b) Crear troncos 802.1Q que utilicen la VLAN 6 nativa

- Procedemos a crear troncos 802.1Q para la interface F0/1 y F0/2.

S1(config)#interface range f0/1-2
S1(config-if-range)#switchport trunk encapsulation dot1q
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2
S1(config-if-range)#switchport trunk allowed vlan 3
S1(config-if-range)#switchport trunk allowed vlan 4
S1(config-if-range)#switchport trunk allowed vlan 5
S1(config-if-range)#switchport trunk allowed vlan 6
S1(config-if-range)#exit

- Procedemos a crear troncos 802.1Q para la interface F0/5.

S1(config)#interface f0/5
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2
S1(config-if)#switchport trunk allowed vlan 3
S1(config-if)#switchport trunk allowed vlan 4
S1(config-if)#switchport trunk allowed vlan 5
S1(config-if)#switchport trunk allowed vlan 6
S1(config-if)#exit

c) Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

- Procedemos a Crear un grupo de puertos EtherChannel de Capa 2.

S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#exit

d) Configurar el puerto de acceso de host para VLAN 2

- Procedemos a configurar el puerto de acceso

S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2

e) Configurar la seguridad del puerto en los puertos de acceso

- Procedemos a configurar la seguridad para los puertos de acceso

S1(config)#interface f0/6
S1(config-if)#switchport port-security maximum 3

f) Proteja todas las interfaces no utilizadas

- Procedemos a proteger las interfaces de la 3 a la 4.

S1(config)#interface range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#

- Procedemos a proteger las interfaces de la 7 a la 24.

S1(config)#interface range f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#

- Procedemos a proteger las interfaces GigabitEthernet0/1-2.

S1(config)#interface range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
S1(config-if-range)#exit
S1(config)#

Paso 5: Configurar el S2

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

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tabla No. 6. Tareas configuración para S2.

a) Crear VLAN

- Se accede al Switch, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  User Access Verification

  Username: admin
  Password:
  S2>enable
  Password:
  S2#

- Procedemos a ingresar al modo de configuración.

  S2#config t
  Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#

- Ahora procedemos a crear las VLAN

S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native

b) Crear troncos 802.1Q que utilicen la VLAN 6 nativa

- Procedemos a crear troncos 802.1Q para la interface F0/1 y F0/2.

S2(config)#interface range f0/1-2
S2(config-if-range)#switchport trunk encapsulation dot1q
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2
S2(config-if-range)#switchport trunk allowed vlan 3
S2(config-if-range)#switchport trunk allowed vlan 4
S2(config-if-range)#switchport trunk allowed vlan 5
S2(config-if-range)#switchport trunk allowed vlan 6
S2(config-if-range)#exit

c) Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

- Procedemos a Crear un grupo de puertos EtherChannel de Capa 2.

S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#exit

d) Configurar el puerto de acceso de host para VLAN 3

- Procedemos a configurar el puerto de acceso

S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3

e) Configurar la seguridad del puerto en los puertos de acceso

- Procedemos a configurar la seguridad para los puertos de acceso

S2(config)#interface f0/18
S2(config-if)#switchport port-security maximum 3

f) Asegure todas las interfaces no utilizadas

- Procedemos a proteger las interfaces de la 3 a la 17.

S2(config)#interface range f0/3-17
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#

- Procedemos a proteger las interfaces de la 19 a la 24.

S2(config)#interface range f0/19-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#

- Procedemos a proteger las interfaces GigabitEthernet0/1-2.

S2(config)#interface range g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
S2(config-if-range)#exit
S2(config)#

PARTE 3: CONFIGURAR SOPORTE DE HOSTS

Paso 6: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Tabla No. 7. Tareas configuración para R1.

a) Configure Default Routing

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  User Access Verification

  Username: admin
  Password:
  R1>enable
  Password:
  R1#

- Procedemos a ingresar al modo de configuración.

  R1#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  R1(config)#

- Procedemos a crear las rutas predeterminadas para los protocolos IPV4 e IPV6 para que dirijan tráfico a la interfaz Loopback 0.

  R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
  %Default route without gateway, if not a point-to-point interface, may impact performance

R1(config)#ipv6 route ::/0 loopback 0
R1(config)#

b) Configurar IPv4 DHCP para VLAN 2

- Procedemos a crear un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool VLAN2-Bikes
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
R1(config)#

c) Configurar DHCP IPv4 para VLAN 3

- Procedemos a crear un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.

R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool VLAN3-Trikes
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit
R1(config)#

Paso 7: 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.

Configuración de red de PC-A	
Descripción	
Dirección física	
Dirección IP	

Configuración de red de PC-A	
Máscara de subred	
Gateway predeterminado	
Gateway predeterminado IPv6	

Tabla No. 8. Configuración de red PC-A.

Configuración de red de PC-B	
Descripción	
Dirección física	
Dirección IP	
Máscara de subred	
Gateway predeterminado	
Gateway predeterminado IPv6	

Tabla No. 9. Configuración de red PC-B.

Configuración equipo hosts PC-A

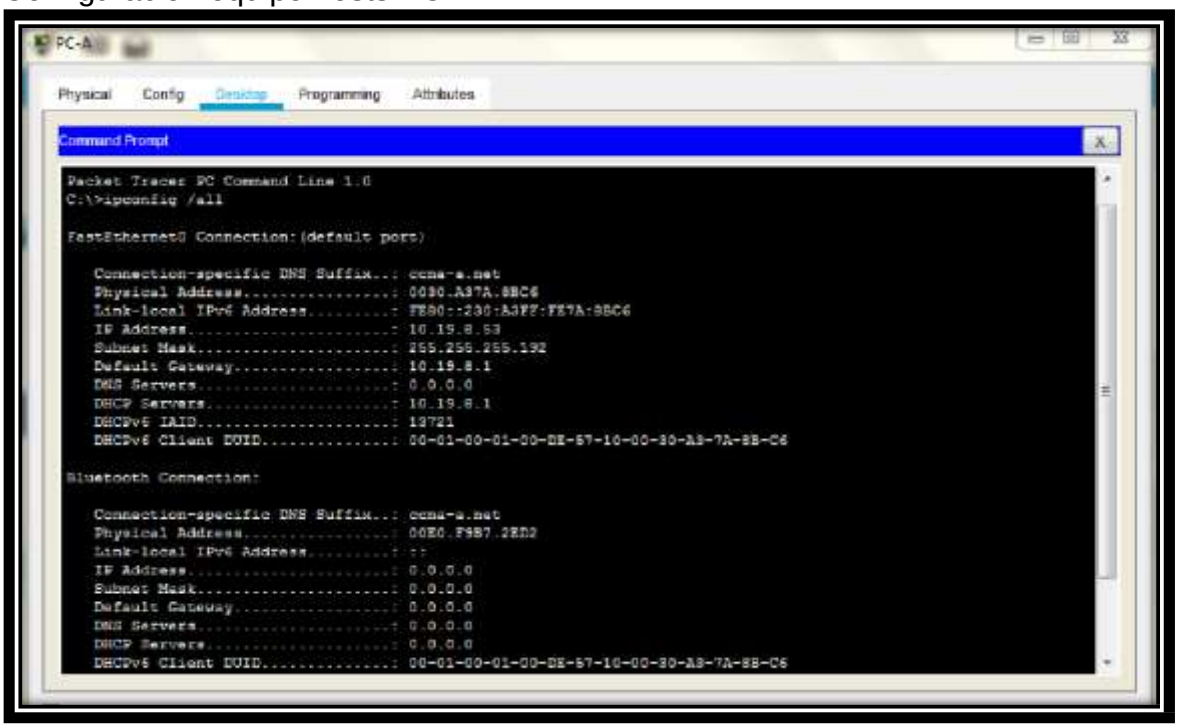

Figura No. 2. Configuración equipo hosts PC-A

Configuración equipo hosts PC-B

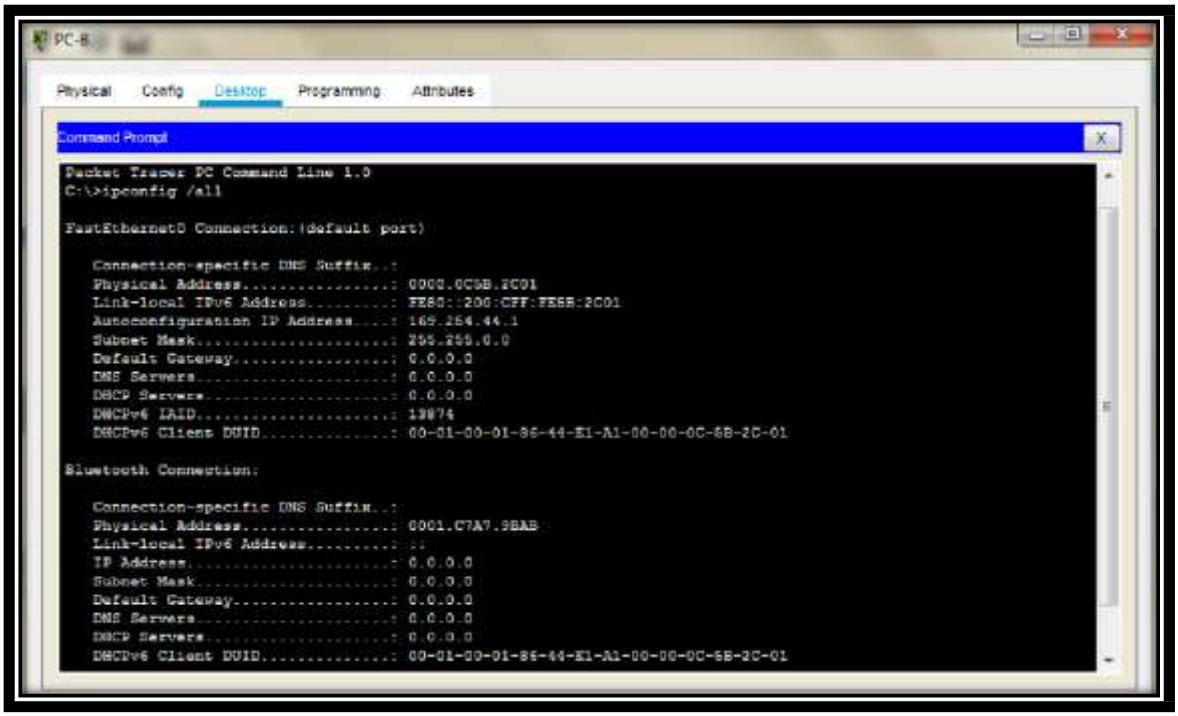

Figura No. 3. Configuración equipo hosts PC-B

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.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

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:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Conectividad Exitosa
		IPv6	2001:db8:acad:a: :1	en blanco
	R1, G0/0/1.3	Dirección	10.19.8.65	en blanco
		IPv6	2001:db8:acad:b: :1	en blanco

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.4	Dirección	10.19.8.97	en blanco
		IPv6	2001:db8:acad:c: :1	en blanco
	S1, VLAN 4	Dirección	10.19.8.98	en blanco
		IPv6	2001:db8:acad:c: :98	en blanco
	S2, VLAN 4	Dirección	10.19.8.99.	en blanco
		IPv6	2001:db8:acad:c: :99	en blanco
	PC-B	Dirección	IP address will vary.	en blanco
		IPv6	2001:db8:acad:b: :50	en blanco
	R1 Bucle 0	Dirección	209.165.201.1	en blanco
		IPv6	2001:db8:acad:209: :1	en blanco
PC-B	R1 Bucle 0	Dirección	209.165.201.1	en blanco
		IPv6	2001:db8:acad:209: :1	en blanco
	R1, G0/0/1.2	Dirección	10.19.8.1	en blanco
		IPv6	2001:db8:acad:a: :1	en blanco
	R1, G0/0/1.3	Dirección	10.19.8.65	en blanco
		IPv6	2001:db8:acad:b: :1	en blanco
	R1, G0/0/1.4	Dirección	10.19.8.97	en blanco
		IPv6	2001:db8:acad:c: :1	en blanco
	S1, VLAN 4	Dirección	10.19.8.98	en blanco
		IPv6	2001:db8:acad:c: :98	en blanco

Desde	A	de Internet	Dirección IP	Resultados de ping
	S2, VLAN 4	Dirección	10.19.8.99.	en blanco
		IPv6	2001:db8:acad:c::99	en blanco

Tabla No. 10. Verificación conectividad de extremo a extremo.

Verificación conectividad de extremo a extremo

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.

Topología

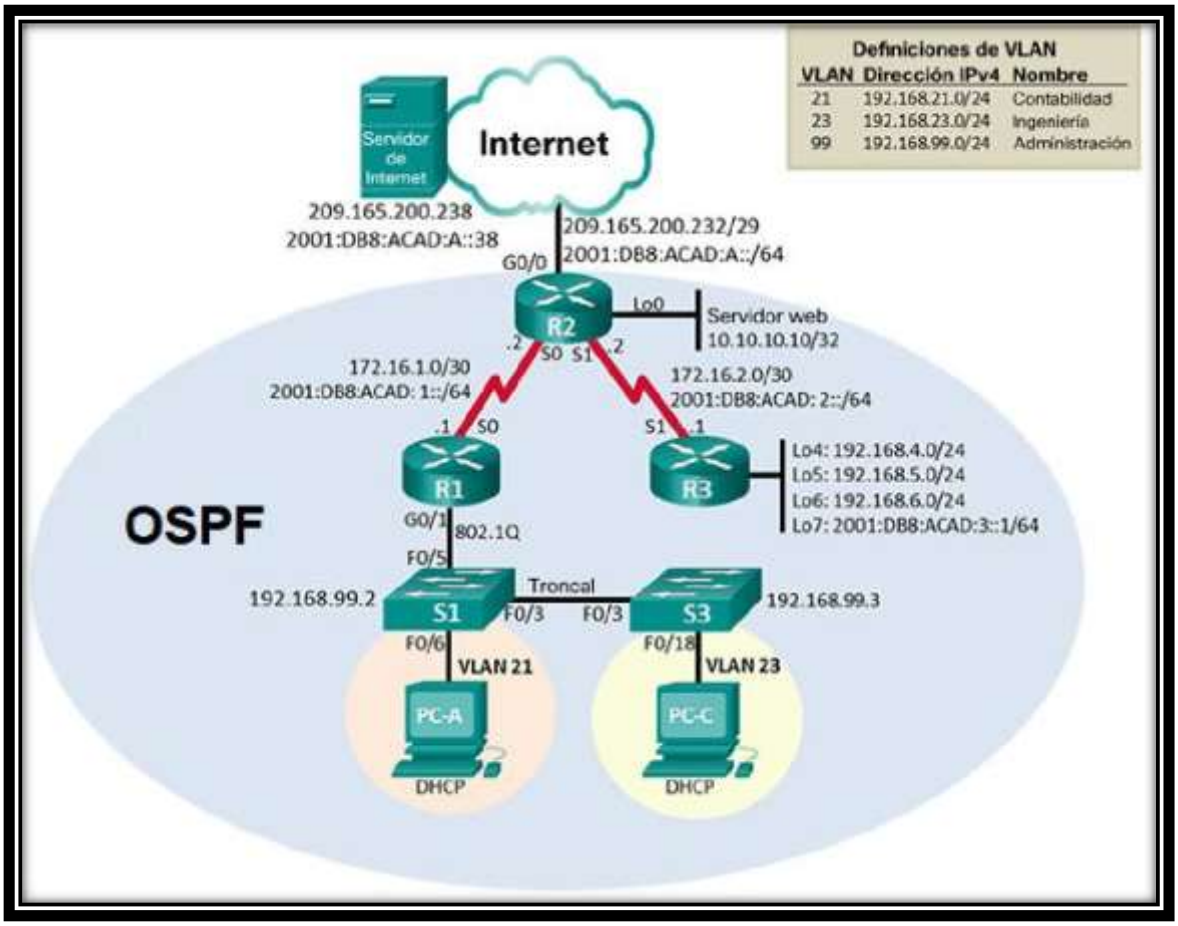

Figura No. 4. Topología de Red Escenario 2

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	**Router#**erase startup-config
Volver a cargar todos los routers	**Router#**reload
Eliminar el archivo startup-config de todos los Switches y eliminar la base de datos de VLAN anterior	**Switch#**erase startup-config **Switch#**delete flash:vlan.dat
Volver a cargar ambos Switches	**Switch#**reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos Switches	**Switch#**show vlan

Tabla No. 11. Comandos IOS inicialización y cargue Routers y Switches.

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 2: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

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
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla No. 12. Configuración Servidor de Internet.

Para realizar la configuración al Servidor de Internet, lo que hacemos es ingresar al Servidor, en la pestaña “Config”, verificamos que los se encuentre seleccionada la opción estática y digitamos la información de acuerdo a la Tabla.

Figura No. 5. Configuración Servidor de Internet

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje 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 Activar la interfaz

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Tabla No. 13. Configuración para R1.

Nota: Todavía no configure G0/1.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  Router> enable
  Router#

- Procedemos a ingresar al modo de configuración.

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

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

  Router(config)#no ip domain-lookup
  Router(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

  Router#show run | include domain-lookup
  no ip domain-lookup
  Router#

- Procedemos a guardar la configuración NVRAM.

  Router#copy run start
  Destination filename [startup-config]?
  Building configuration...
  [OK]

Router#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Router mediante el comando “hostname R1”, damos Enter y salimos del modo de configuración.

Router(config)#hostname R1
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

c) Contraseña de EXEC privilegiado cifrada

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

R1(config)#enable secret class
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

d) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

R1(config)#line console 0
R1(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#

e) Contraseña de acceso Telnet

- Ahora, procedemos a crear la contraseña de acceso a Telnet

  R1(config)#line vty 0 4
  R1(config-line)#password cisco
  R1(config-line)#login
  R1(config-line)#exit
  R1(config)#

f) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

  R1(config)#service password-encryption
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console
  R1#

g) Mensaje MOTD

- Procedemos a ingresar el mensaje de acceso al Router

  R1(config)#banner motd "Se prohíbe el acceso no autorizado"
  R1(config)#

h) Habilitar el routing IPv6

- Procedemos a realizar la activación del protocolo IPV6 a nivel global.

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

i) Interfaz S0/0/0

- Procedemos a ingresar a la interfaz S0/0/0, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

  R1(config)#interface serial 0/1/0
  R1(config-if)#description R1 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 shutdown

R1(config-if)#exit

j) Rutas predeterminadas

- Procedemos a configurar las rutas predeterminadas para IPV4 e IPV6.

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
R1(config)#ipv6 route ::/0 s0/1/0
R1(config)#ipv6 unicas
R1(config)#ipv6 unicast-routing

Paso 4: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	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

Interfaz S0/0/1	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 direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Tabla No. 14. Configuración para R2.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  Router> enable
  Router#

- Procedemos a ingresar al modo de configuración.

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

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

Router(config)#no ip domain-lookup
Router(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

Router#show run | include domain-lookup
no ip domain-lookup
Router#

- Procedemos a guardar la configuración NVRAM.

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Router mediante el comando “hostname R2”, damos Enter y salimos del modo de configuración.

Router(config)#hostname R2
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

c) Contraseña de EXEC privilegiado cifrada

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

R2(config)#enable secret class
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#

d) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

  R2(config)#line console 0
  R2(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

  R2(config-line)#password cisco
  R2(config-line)#login
  R2(config-line)#exit
  R2(config)#exit
  R2#
  %SYS-5-CONFIG_I: Configured from console by console
  R2#

e) Contraseña de acceso Telnet

- Ahora, procedemos a crear la contraseña de acceso a Telnet

  R2(config)#line vty 0 4
  R2(config-line)#password cisco
  R2(config-line)#login
  R2(config-line)#exit
  R2(config)#

f) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

  R2(config)#service password-encryption
  R2(config)#exit
  R2#
  %SYS-5-CONFIG_I: Configured from console by console
  R2#

g) Habilitar el servidor HTTP

- Procedemos a realizar la habilitación para Servidor HTTP.

  R2(config)#ip http server
  R2(config)#ip http secure-server
  R2(config)#ip http authentication local

h) Mensaje MOTD

- Procedemos a ingresar el mensaje de acceso al Router

R2(config)#banner motd "Se prohíbe el acceso no autorizado"
R2(config)#

i) Habilitar el routing IPv6

- Procedemos a realizar la activación del protocolo IPV6 a nivel global.

R2(config)#ipv6 unicast-routing
R2(config)#

j) Interfaz S0/1/0

- Procedemos a ingresar a la interfaz S0/1/0, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R2(config)#interface serial 0/1/0
R2(config-if)#description R1 a R2
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
R2(config-if)#exit

k) Interfaz S0/1/1

- Procedemos a ingresar a la interfaz S0/1/1, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R2(config)#interface serial 0/1/1
R2(config-if)#description R2 a 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
R2(config-if)#exit

l) Interfaz G0/0 (simulación de Internet)

- Procedemos a ingresar a la interfaz G0/0, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R2(config)# interface gigabitEthernet 0/0
R2(config-if)# description R2 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
R2(config-if)#exit

m) Interfaz loopback 0 (servidor web simulado)

- Procedemos a ingresar a la interfaz loopback 0, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R2(config)# interface lo0
R2(config-if)# ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit

n) Rutas predeterminadas

- Procedemos a configurar las rutas predeterminadas para IPV4 e IPV6.

R2(config)# ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0
R2(config)# ipv6 route ::/0 gigabitEthernet 0/0
R2(config)#ipv6 unicas
R2(config)#ipv6 unicast-routing

Paso 5: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	

Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	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
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Tabla No. 15. Configuración para R3.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  Router> enable
  Router#

- Procedemos a ingresar al modo de configuración.

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

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

  Router(config)#no ip domain-lookup
  Router(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y

presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

Router#show run | include domain-lookup
no ip domain-lookup
Router#

- Procedemos a guardar la configuración NVRAM.

Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Router mediante el comando “hostname R3”, damos Enter y salimos del modo de configuración.

Router(config)#hostname R3
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

c) Contraseña de EXEC privilegiado cifrada

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

R3(config)#enable secret class
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

d) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

R3(config)#line console 0

R3(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

e) Contraseña de acceso Telnet

- Ahora, procedemos a crear la contraseña de acceso a Telnet

R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#

f) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

R3(config)#service password-encryption
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

g) Mensaje MOTD

- Procedemos a ingresar el mensaje de acceso al Router

R3(config)#banner motd "Se prohíbe el acceso no autorizado"
R3(config)#

h) Habilitar el routing IPv6

- Procedemos a realizar la activación del protocolo IPV6 a nivel global.

R3(config)#ipv6 unicast-routing
R3(config)#

i) Interfaz S0/1/0

- Procedemos a ingresar a la interfaz S0/1/0, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R3(config)#interface serial 0/1/0
R3(config-if)#description R3 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
R3(config-if)#exit

j) Interfaz loopback 4

- Procedemos a ingresar a la interfaz loopback 4, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R3(config)# interface lo4
R3(config-if)# ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit

k) Interfaz loopback 5

- Procedemos a ingresar a la interfaz loopback 5, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R3(config)# interface lo5
R3(config-if)# ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit

l) Interfaz loopback 6

- Procedemos a ingresar a la interfaz loopback 6, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R3(config)# interface lo6
R3(config-if)# ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit

m) Interfaz loopback 7

- Procedemos a ingresar a la interfaz loopback 7, para realizar las respectivas configuraciones de acuerdo al diagrama de topología.

R3(config)# interface lo7
R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ipv6 unicast-routing

n) Rutas predeterminadas

- Procedemos a configurar las rutas predeterminadas para IPV4 e IPV6.

R3(config)# ip route 0.0.0.0 0.0.0.0 s0/1/1
R3(config)# ipv6 route ::/0 s0/1/1
R3(config)#ipv6 unicas
R3(config)#ipv6 unicast-routing

Paso 6: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla No. 16. Configuración para S1.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

Switch> enable
Switch#

- Procedemos a ingresar al modo de configuración.

  Switch#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  Switch(config)#

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

  Switch(config)#no ip domain-lookup
  Switch(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

  Switch#show run | include domain-lookup
  no ip domain-lookup
  Switch#

- Procedemos a guardar la configuración NVRAM.

  Switch#copy run start
  Destination filename [startup-config]?
  Building configuration...
  [OK]
  Switch#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Switch mediante el comando “hostname S1”, damos Enter y salimos del modo de configuración.

  Switch(config)#hostname S1
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

c) Contraseña de EXEC privilegiado cifrada

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

  S1(config)#enable secret class
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

d) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

  S1(config)#line console 0
  S1(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

  S1(config-line)#password cisco
  S1(config-line)#login
  S1(config-line)#exit
  S1(config)#exit
  S1#
  %SYS-5-CONFIG_I: Configured from console by console
  S1#

e) Contraseña de acceso Telnet

- Ahora, procedemos a crear la contraseña de acceso a Telnet

  S1(config)#line vty 0 4
  S1(config-line)#password cisco
  S1(config-line)#login
  S1(config-line)#exit
  S1(config)#

f) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

  S1(config)#service password-encryption

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

g) Mensaje MOTD

- Procedemos a ingresar el mensaje de acceso al Router

S1(config)#banner motd "Se prohíbe el acceso no autorizado"
S1(config)#

Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Tabla No. 17. Configuración para S3.

a) Desactivar la búsqueda DNS

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

Switch> enable
Switch#

- Procedemos a ingresar al modo de configuración.

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

- Procedemos a digitar el comando “no ip domain-lookup” y presionamos enter.

Switch(config)#no ip domain-lookup
Switch(config)#

- Procedemos a digitar la palabra “exit” para salir del modo de configuración, y escribimos “show run | include domain-lookup” y presionamos Enter, por lo que nos debe salir una línea que diga "no ip domain-lookup"; lo que comprueba que la configuración esta activa.

Switch#show run | include domain-lookup
no ip domain-lookup
Switch#

- Procedemos a guardar la configuración NVRAM.

Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#

b) Nombre del router

- En el modo de configuración lo que hacemos es dar nombre al Switch mediante el comando “hostname S3”, damos Enter y salimos del modo de configuración.

Switch(config)#hostname S3
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

c) Contraseña de EXEC privilegiado cifrada

- Procedemos a establecer la contraseña para el modo EXEC privilegiado y salimos del modo de configuración.

S3(config)#enable secret class

S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#

d) Contraseña de acceso a la consola

- Procedemos a ingresar a la línea de Consola, que es donde registraremos la contraseña de acceso a consola.

  S3(config)#line console 0
  S3(config-line)#

- Procedemos a establecer la contraseña para el acceso a la consola y salimos del modo de configuración.

  S3(config-line)#password cisco
  S3(config-line)#login
  S3(config-line)#exit
  S3(config)#exit
  S3#
  %SYS-5-CONFIG_I: Configured from console by console
  S3#

e) Contraseña de acceso Telnet

- Ahora, procedemos a crear la contraseña de acceso a Telnet

  S3(config)#line vty 0 4
  S3(config-line)#password cisco
  S3(config-line)#login
  S3(config-line)#exit
  S3(config)#

f) Cifrar las contraseñas de texto no cifrado

- Procedemos a digitar el comando para cifrar todas las contraseñas.

  S3(config)#service password-encryption
  S3(config)#exit
  S3#
  %SYS-5-CONFIG_I: Configured from console by console
  S3#

g) Mensaje MOTD

- Procedemos a ingresar el mensaje de acceso al Router

S1(config)#banner motd "Se prohíbe el acceso no autorizado"
S1(config)#

Paso 8: 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:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/19 ms
R2	R3, S0/1/1	172.16.2.1	Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC de Internet	Gateway predeterminado	209.165.200.233	

Tabla No. 18. Verificación conectividad de la red.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Resultado Ping R1 a R2, S0/1/0

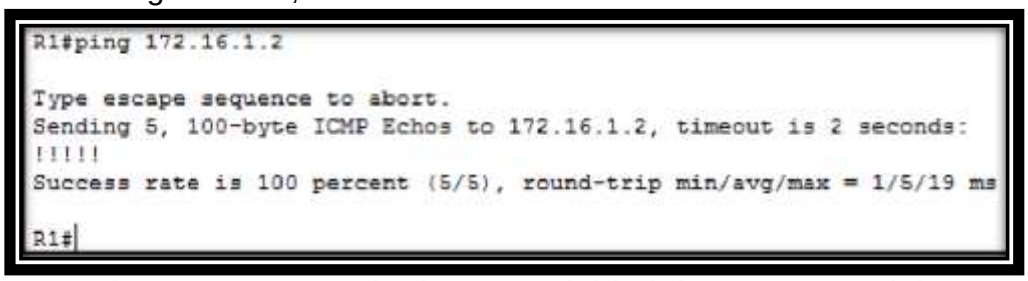

Figura No. 6. Resultado Conectividad de R1 a R2, S0/1/0

Resultado Ping R2 a R3, S0/1/1

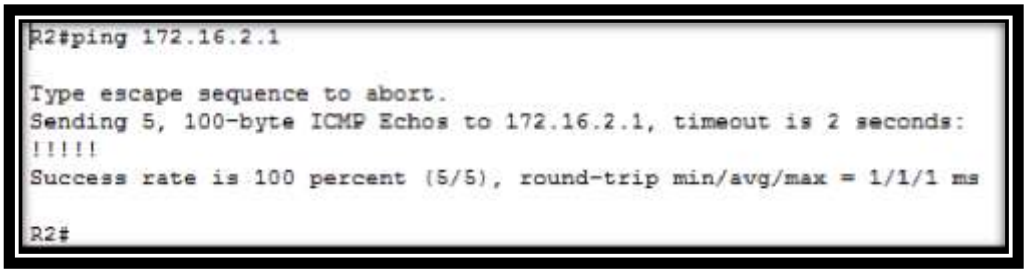

Figura No. 7. Resultado Conectividad de R2 a R3, S0/1/1

Resultado Ping Servidor de Internet a Gateway predeterminado

PARTE 3: CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

Paso 9: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Tabla No. 19. Configuración del S1

a) Crear la base de datos de VLAN

- Se accede al Switch, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  S1> enable
  S1#

- Procedemos a ingresar al modo de configuración.

  S1#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  S1(config)#

- Procedemos a crear y nombrar cada una de las VLAN tal cual se indica en la topología de la red.

  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 Administracion
  S1(config-vlan)#exit
  S1(config)#

b) Asignar la dirección IP de administración.

- Procedemos a realizar la asignación de la dirección IP para Administración.

  S1(config)#interface vlan 99
  S1(config-if)#
  %LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#

c) Asignar el Gateway predeterminado

- Procedemos a realizar la asignación del Gateway

S1(config)#ip default-gateway 192.168.99.1

d) Forzar el enlace troncal en la interfaz F0/3

- Procedemos a realizar el forzamiento en el enlace troncal de la interfaz F0/3.

S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#

e) Forzar el enlace troncal en la interfaz F0/5

- Procedemos a realizar el forzamiento en el enlace troncal de la interfaz F0/5.

S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#

f) Configurar el resto de los puertos como puertos de acceso

- Procedemos a configurar los puertos para que sean de acceso.

  S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24
  S1(config-if-range)#switchport mode access
  S1(config-if-range)#exit
  S1(config)#

g) Asignar F0/6 a la VLAN 21

- Procedemos a realizar la asignación de F0/6 a la VLAN 21

  S1(config)#interface range fa0/6
  S1(config-if-range)#switchport access vlan 21
  S1(config-if-range)#exit
  S1(config)#

h) Apagar todos los puertos sin usar

- Procedemos a apagar los puertos que no se están utilizando

  S1(config)#interface range fa0/1-2,fa0/4,fa0/7-24,gi0/1-2
  S1(config-if-range)#shutdown
  S1(config-if-range)#exit
  S1(config)#

Paso 10: Configurar S3

La configuración del S3 incluye las siguientes tareas:

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.
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
Asignar el gateway predeterminado.	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

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	
Apagar todos los puertos sin usar	

Tabla No. 20. Configuración de S3

a) Crear la base de datos de VLAN

- Se accede al Switch, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  S3> enable
  S3#

- Procedemos a ingresar al modo de configuración.

  S3#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  S3(config)#

- Procedemos a crear y nombrar cada una de las VLAN tal cual se indica en la topología de la red.

  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 Administracion
  S3(config-vlan)#exit
  S3(config)#

b) Asignar la dirección IP de administración.

- Procedemos a realizar la asignación de la dirección IP para Administración.

  S3(config)#interface vlan 99
  S3(config-if)#
  %LINK-5-CHANGED: Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#

c) Asignar el Gateway predeterminado

- Procedemos a realizar la asignación del Gateway

S3(config)#ip default-gateway 192.168.99.1

d) Forzar el enlace troncal en la interfaz F0/3

- Procedemos a realizar el forzamiento en el enlace troncal de la interfaz F0/3.

S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
S3(config)#

e) Configurar el resto de los puertos como puertos de acceso

- Procedemos a configurar los puertos para que sean de acceso.

S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#

f) Asignar F0/18 a la VLAN 21

- Procedemos a realizar la asignación de F0/6 a la VLAN 21

S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
S3(config)#

g) Apagar todos los puertos sin usar

- Procedemos a apagar los puertos que no se están utilizando

S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2

S3(config-if-range)#shutdown
S3(config-if-range)#exit
S3(config)#

Paso 11: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Tabla No. 21. Configuración de R1

a) Configurar la subinterfaz 802.1Q .21 en G0/1

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R1> enable
R1#

- Procedemos a ingresar al modo de configuración.

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#

- Procedemos a realizar la configuración de la subinterfaz 802.1Q .21 en G0/1

R1(config)#interface gigabitEthernet 0/1.21
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
R1(config-subif)#exit
R1(config)#

b) Configurar la subinterfaz 802.1Q .23 en G0/1

- Procedemos a realizar la configuración de la subinterfaz 802.1Q .23 en G0/1

R1(config)#interface gigabitEthernet 0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#

c) Configurar la subinterfaz 802.1Q .99 en G0/1

- Procedemos a realizar la configuración de la subinterfaz 802.1Q .99 en G0/1

R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#

d) Activar la interfaz G0/1

- Procedemos a realizar la activación de la Interfaz G0/1

R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
R1(config-if)#exit

Paso 12: 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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3	R1, dirección VLAN 99	192.168.99.1	Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1	R1, dirección VLAN 21	192.168.21.1	Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip

			min/avg/max = 0/0/1 ms

Tabla No. 22. Verificación conectividad de la Red.

Verificación conectividad desde S1 a R1, dirección VLAN 99

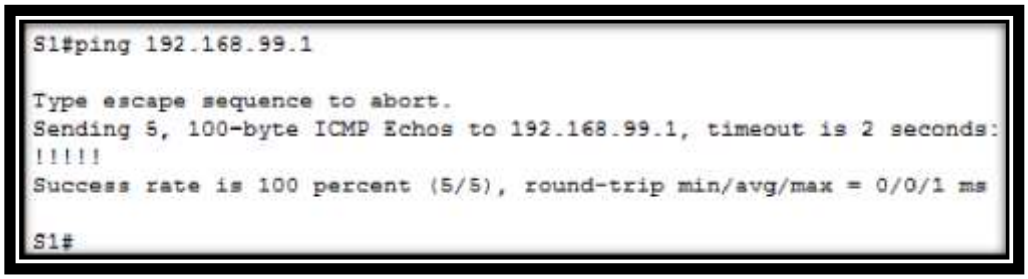

Figura No. 8. Conectividad desde S1 a R1, dirección VLAN 99

Verificación conectividad desde S3 a R1, dirección VLAN 99

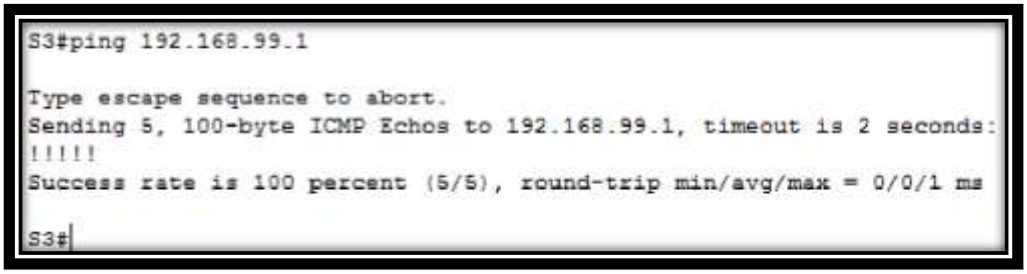

Figura No. 9. Conectividad desde S3 a R1, dirección VLAN 99

Verificación conectividad desde S1 a R1, dirección VLAN 21

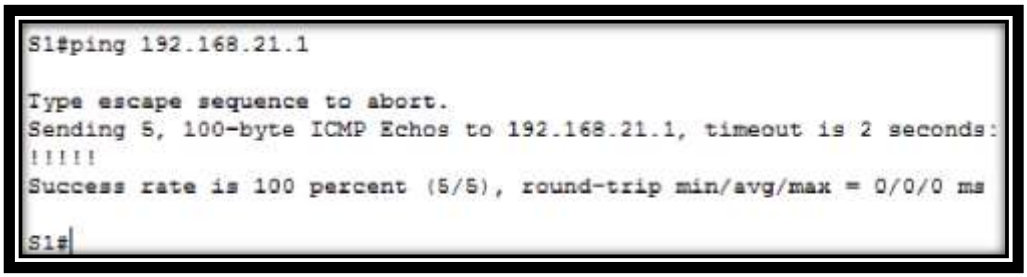

Figura No. 10. Conectividad desde S1 a R1, dirección VLAN 21

Verificación conectividad desde S3 a R1, dirección VLAN 23

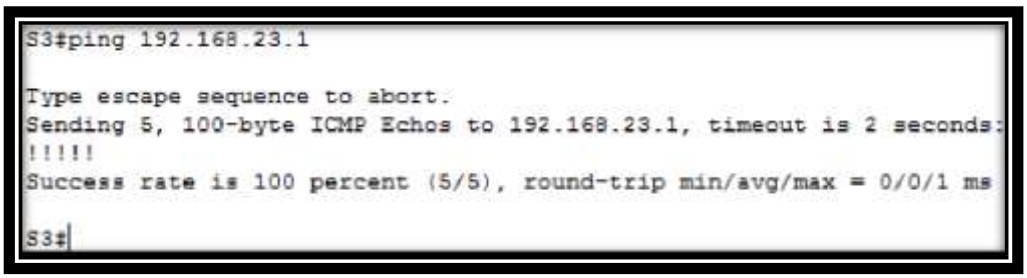

Figura No. 11. Conectividad desde S3 a R1, dirección VLAN 23

PARTE 4: CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

Paso 13: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Tabla No. 23. Configuración OSPF en el R1.

a) Configurar OSPF área 0

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R1> enable
R1#

- Procedemos a ingresar al modo de configuración.

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#

- Se procede a realizar la configuración de OSPF para área 0.

R1(config)#router ospf 1
R1(config-router)#

b) Anunciar las redes conectadas directamente

- Se procede a anunciar las redes conectadas directamente.

R1(config-router)#do show ip route c
C 172.16.1.0/30 is directly connected, Serial0/1/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1(config-router)#

R1(config-router)#network 172.16.1.0 255.255.255.252 area 0
R1(config-router)#network 192.168.21.0 255.255.255.0 area 0
R1(config-router)#network 192.168.23.0 255.255.255.0 area 0
R1(config-router)#network 192.168.99.0 255.255.255.0 area 0
R1(config-router)#

c) Establecer todas las interfaces LAN como pasivas

- Se procede a establecer todas las interfaces LAN como pasivas.

R1(config-router)#passive-interface gigabitEthernet0/1.21
R1(config-router)#passive-interface gigabitEthernet0/1.23
R1(config-router)#passive-interface gigabitEthernet0/1.99
R1(config-router)#

d) Desactive la sumarización automática

- Procedemos a realizar la desactivación de la sumarización automática

R1(config-router)#area 1 stub no-summary

Paso 14: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Tabla No. 24. Configuración OSPF en el R2.

a) Configurar OSPF área 0

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R2> enable

R2#

- Procedemos a ingresar al modo de configuración.

  R2#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  R2(config)#

- Se procede a realizar la configuración de OSPF para área 0.

  R1(config)#router ospf 1
  R1(config-router)#

b) Anunciar las redes conectadas directamente

- Se procede a anunciar las redes conectadas directamente.

  R2(config-router)#do show ip route c
  C 10.10.10.10/32 is directly connected, Loopback0
  C 172.16.1.0/30 is directly connected, Serial0/1/0
  C 172.16.2.0/30 is directly connected, Serial0/1/1
  C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

  R2(config-router)#

  R2(config-router)#network 10.10.10.10 255.255.255.255 area 0
  R2(config-router)#network 172.16.1.0 255.255.255.252 area 0
  R2(config-router)#network 172.16.2.0 255.255.255.252 area 0
  R2(config-router)#

c) Establecer la interfaz LAN (loopback) como pasiva

- Se procede a establecer la interfaz LAN (loopback) como pasiva.

  R2(config-router)#passive-interface lo0
  R2(config-router)#

d) Desactive la sumarización automática

- Procedemos a realizar la desactivación de la sumarización automática

  R2(config-router)#area 1 stub no-summary
  R2(config-router)#

Paso 15: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Tabla No. 25. Configuración OSPF en el R3.

a) Configurar OSPF área 0

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R3> enable
R3#

- Procedemos a ingresar al modo de configuración.

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#

- Se procede a realizar la configuración de OSPF para área 0.

R3(config)#router ospf 1
R3(config-router)#

b) Anunciar las redes conectadas directamente

- Se procede a anunciar las redes conectadas directamente.

R3(config-router)#do show ip route c
C 172.16.2.0/30 is directly connected, Serial0/1/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6

R3(config-router)#

R3(config-router)#network 172.16.2.0 255.255.255.252 area 0
R3(config-router)#network 192.168.4.0 255.255.255.0 area 0

R3(config-router)#network 192.168.5.0 255.255.255.0 area 0
R3(config-router)#network 192.168.6.0 255.255.255.0 area 0
R3(config-router)#

c) Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

- Se procede a establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas.

R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#

d) Desactive la sumarización automática

- Procedemos a realizar la desactivación de la sumarización automática

R3(config-router)#area 1 stub no-summary
R3(config-router)#

Paso 16: Verificar la información de OSPF

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

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 database

Tabla No. 26. Verificación de la información de OSPF.

Verificación comando Show ip protocols

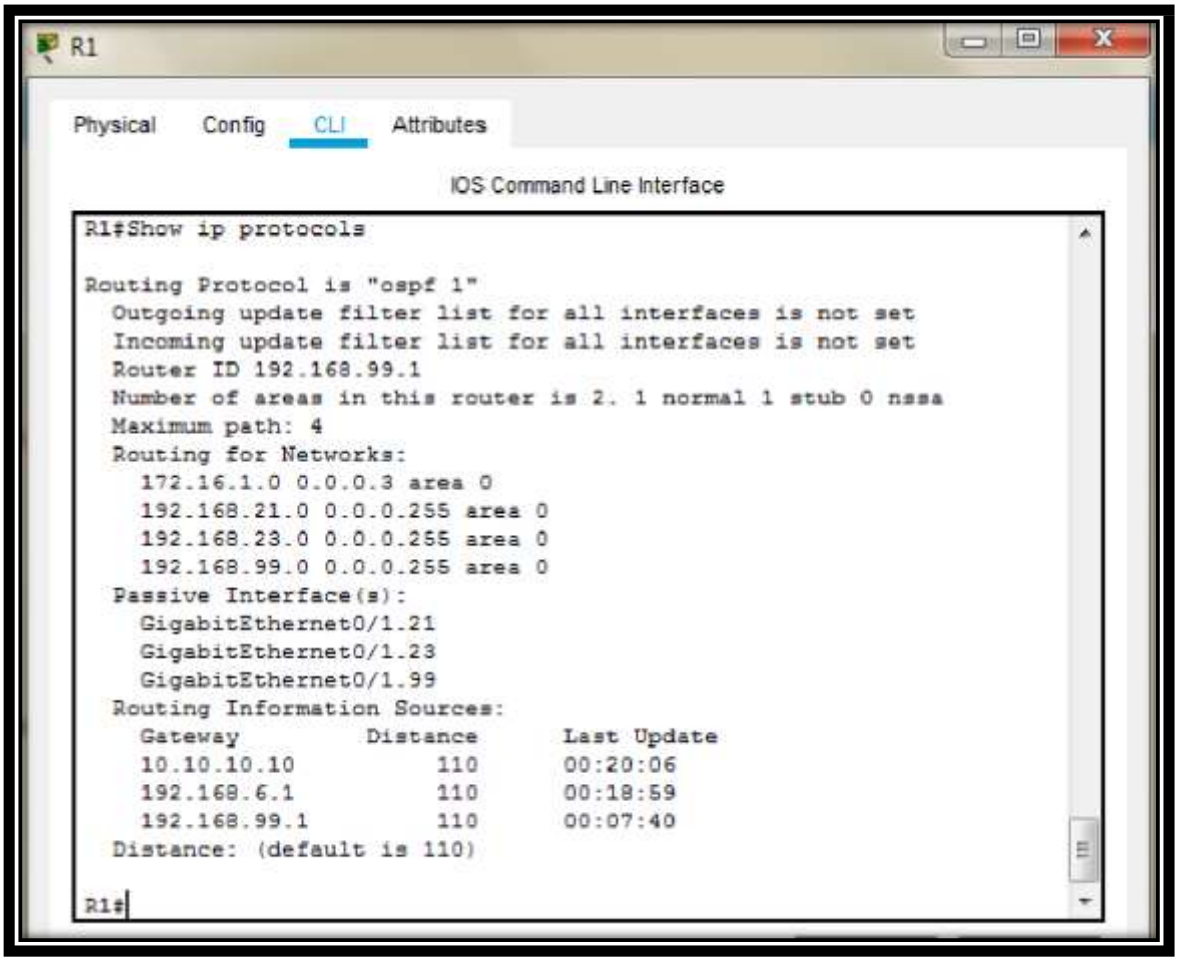

Figura No. 12. Verificación comando Show ip protocols

Verificación comando Show ip route ospf

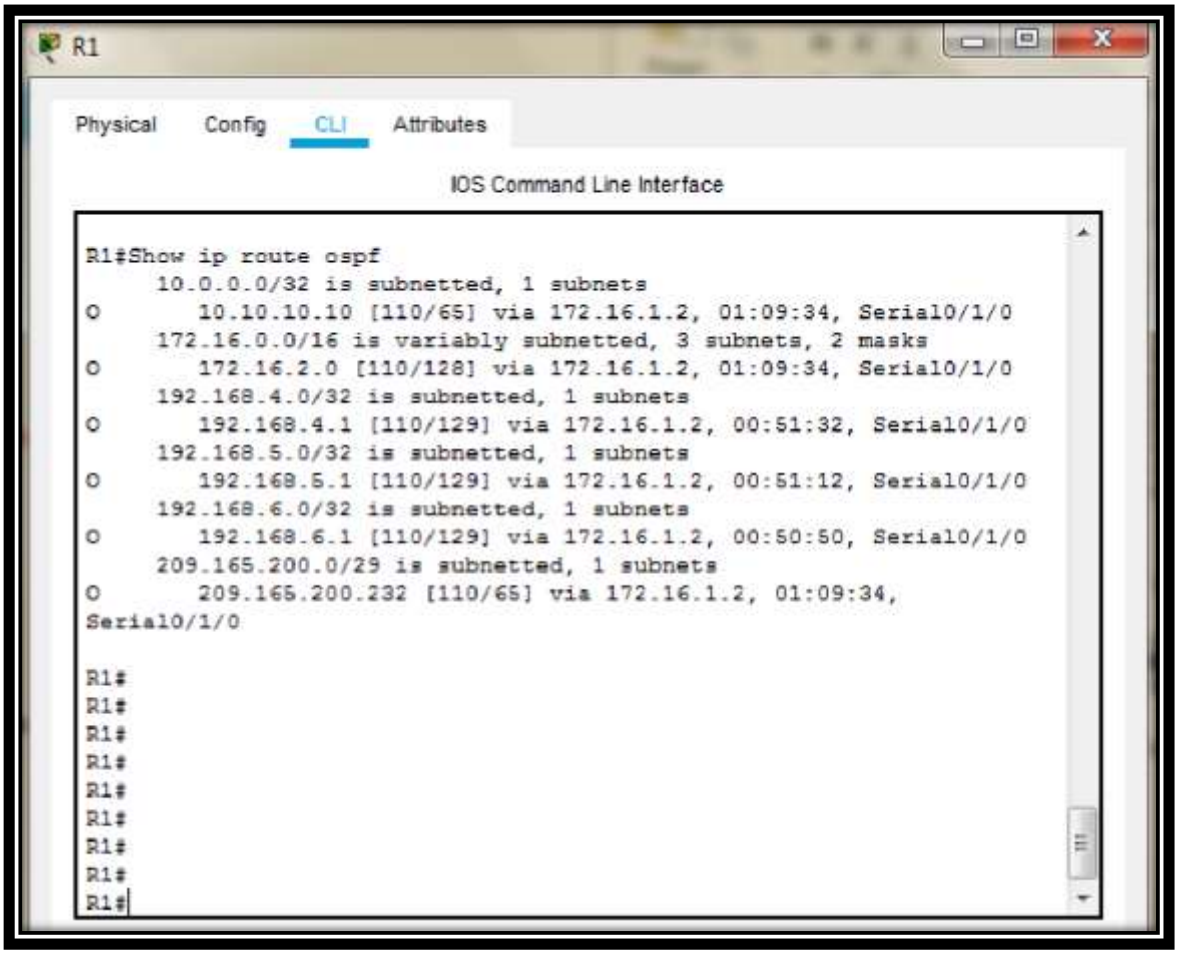

Figura No. 13. Verificación comando Show ip route ospf

Verificación comando Show ip ospf database

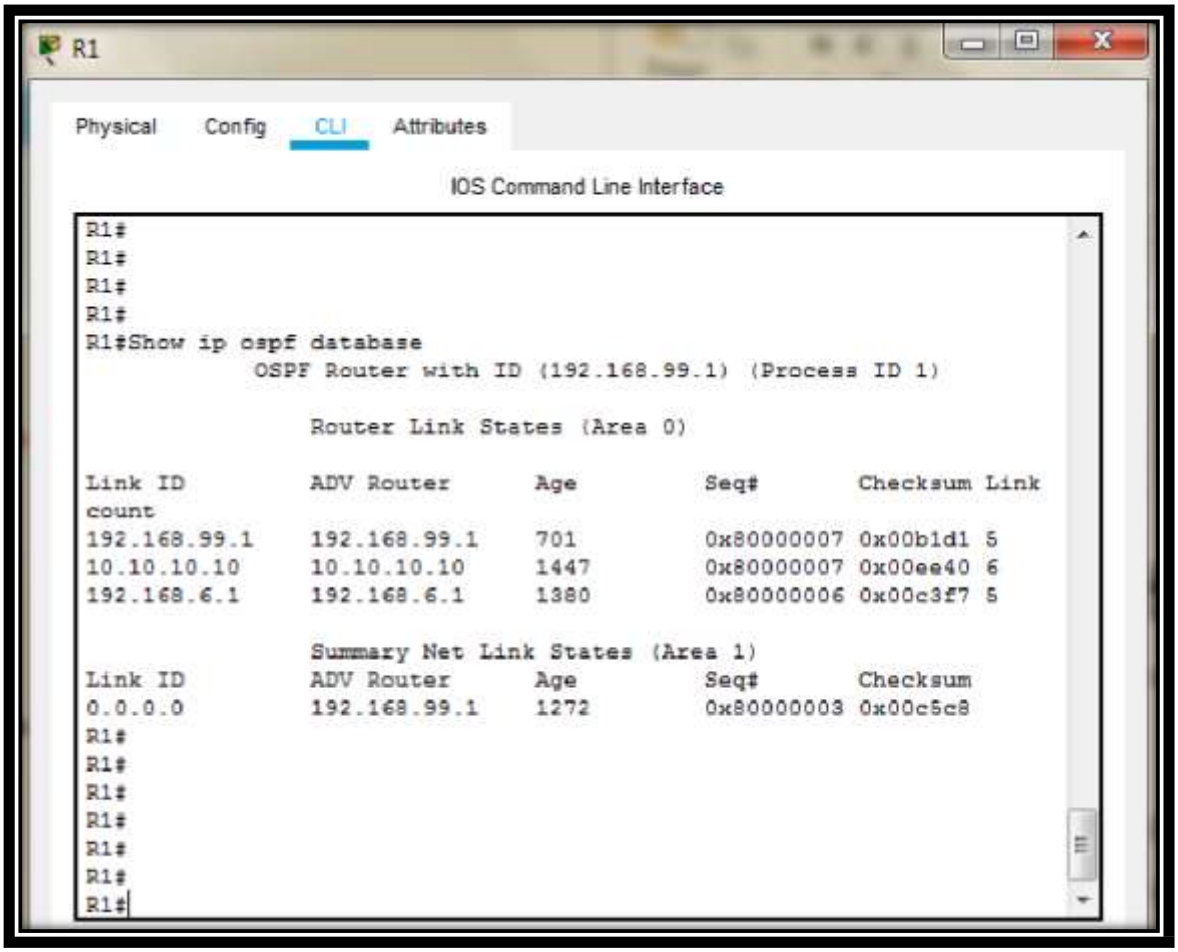

Figura No. 14. Verificación comando Show ip ospf database

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

Paso 17: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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

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

Tabla No. 27. Configuración del R1 como servidor de DHCP para las VLAN 21 y 23.

a) Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R1> enable
R1#

- Procedemos a ingresar al modo de configuración.

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#

- Procedemos a reservar las primeras 20 direcciones para configuraciones estáticas.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#

b) Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

- Procedemos a reservar las primeras 20 direcciones para configuraciones estáticas.

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#

c) Crear un pool de DHCP para la VLAN 21.

- Procedemos a crear un pool de DHCP para la VLAN 21.
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1

R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#

d) Crear un pool de DHCP para la VLAN 23

- Procedemos a crear un pool de DHCP para la VLAN 23.

R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#

Paso 18: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**

Definir la traducción de NAT dinámica	

Tabla No. 28. Configuración NAT estática y dinámica en el R2.

a) Crear una base de datos local con una cuenta de usuario

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R2> enable
R2#

- Procedemos a ingresar al modo de configuración.

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#

- Procedemos a crear una base de datos local con una cuenta de usuario.

R2(config)#user webuser privilege 15 secret cisco 12345
R2(config)#

b) Habilitar el servicio del servidor HTTP

No soportado en Packet Tracer

c) Configurar el servidor HTTP para utilizar la base de datos local para la autenticación

No soportado en Packet Tracer

d) Crear una NAT estática al servidor web.

- Procedemos a crear una NAT estática al servidor Web

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#

e) Asignar la interfaz interna y externa para la NAT estática

- Procedemos a asignar la interfaz interna y externa para la NAT estática.

R2(config)#interface gi0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface serial0/1/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface serial0/1/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#

f) Configurar la NAT dinámica dentro de una ACL privada

- Procedemos a configurar la NAT dinámica dentro de la ACL privada.

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 0.0.0.255
R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
R2(config)#

g) Defina el pool de direcciones IP públicas utilizables.

- Procedemos a definir el pool de direcciones IP publicas utilizables

R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#

h) Definir la traducción de NAT dinámica

- Procedemos a definir la traducción de NAT dinámica.

R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#

Paso 19: 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 correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping statistics for 192.168.21.22: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms
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**	

Tabla No. 29. Verificación del protocolo DHCP y la NAT estática.

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

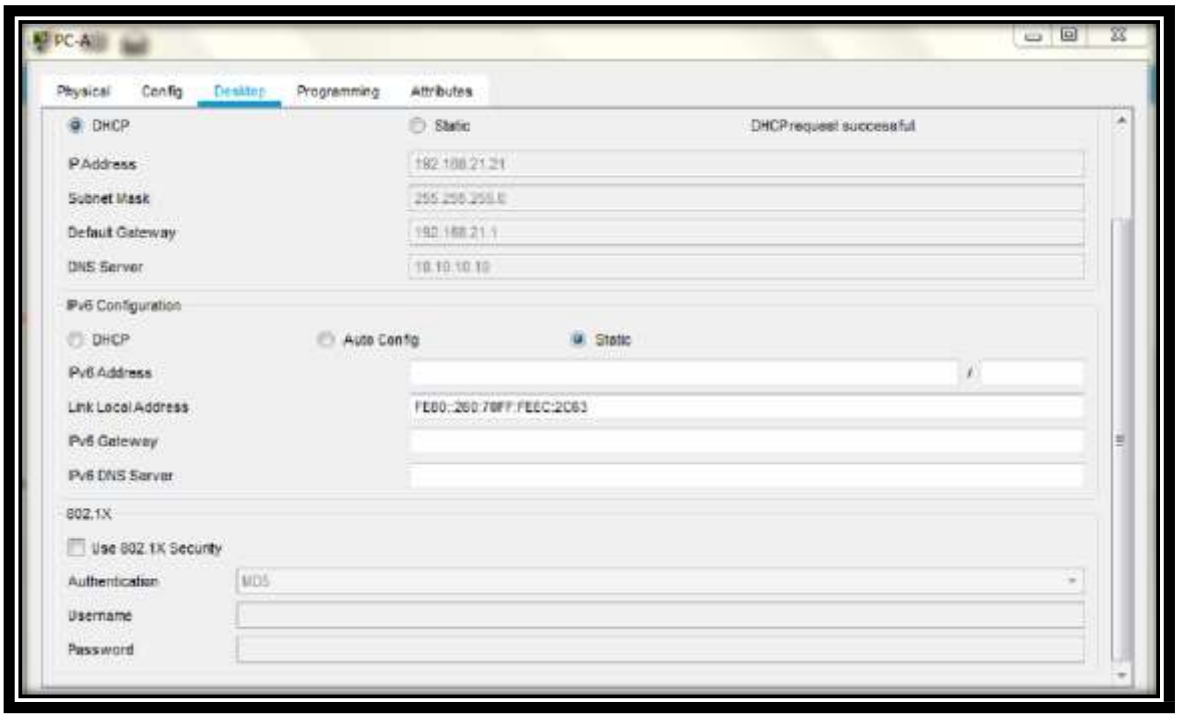

Figura No. 15. Verificación información PC-A – IP del servidor DHCP

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

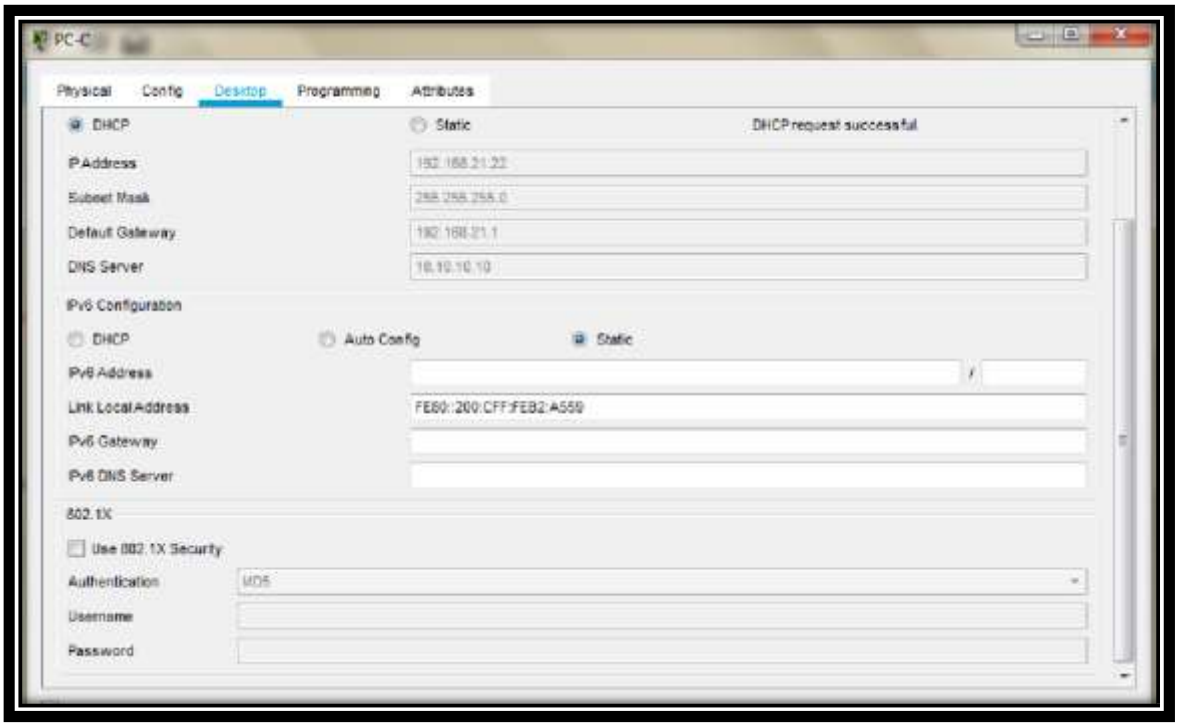

Figura No. 16. Verificación información PC-C – IP del servidor DHCP

Verificar que la PC-A pueda hacer ping a la PC-C

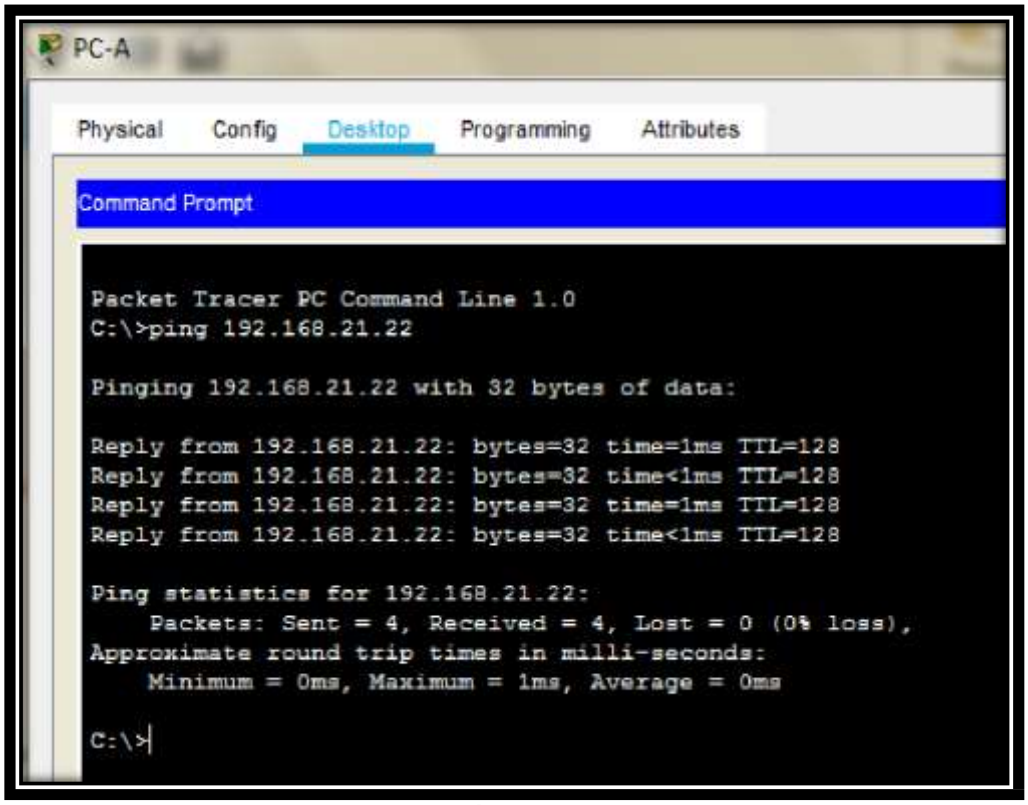

Figura No. 17. Verificación Conectividad PC-A al PC-C

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229)

PARTE 6: CONFIGURAR NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Tabla No. 30. Configuración NTP

a) Ajuste la fecha y hora en R2.

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R2> enable
R2#

- Procedemos a realizar el ajuste de la fecha y hora para R2

R2#clock set 09:00:00 5 Mar 2016
R2#

b) Configure R2 como un maestro NTP.

- Procedemos a ingresar al modo de configuración.

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#

- Procedemos a realizar la configuración de R2 como un maestro NTP

R2(config)#ntp master 5
R2(config)#

c) Configurar R1 como un cliente NTP.

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R1> enable
R1#

- Procedemos a ingresar al modo de configuración.

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#

- Procedemos a realizar la configuración de R1 como un cliente NTP.

R1(config)#ntp server 172.16.1.2
R1(config)#

d) Configure R1 para actualizaciones de calendario periódicas con hora NTP.

- Procedemos a realizar la configuración en R1 para que se ejecuten actualizaciones periódicas al calendario con hora NTP.

  R1(config)#ntp update-calendar
  R1(config)#

e) Verifique la configuración de NTP en R1.

- Procedemos a realizar la verificación de la configuración de NTP en R1.

  R1#show ntp status
  Clock is synchronized, stratum 6, reference is 172.16.1.2
  nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
  reference time is DA603D47.00000305 (9:37:11.773 UTC sáb mar 5 2016)
  clock offset is 0.00 msec, root delay is 4.00 msec
  root dispersion is 10.21 msec, peer dispersion is 0.12 msec.
  loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000001193 s/s system poll interval is 4, last update was 5 sec ago.
  R1#

  R1#show ntp associations

  address ref clock st when poll reach delay offset disp
  *~172.16.1.2 127.127.1.1 5 10 16 377 4.00 0.00 0.12
  * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
  R1#

  R1#show clock
  9:39:30.988 UTC Sat Mar 5 2016
  R1#

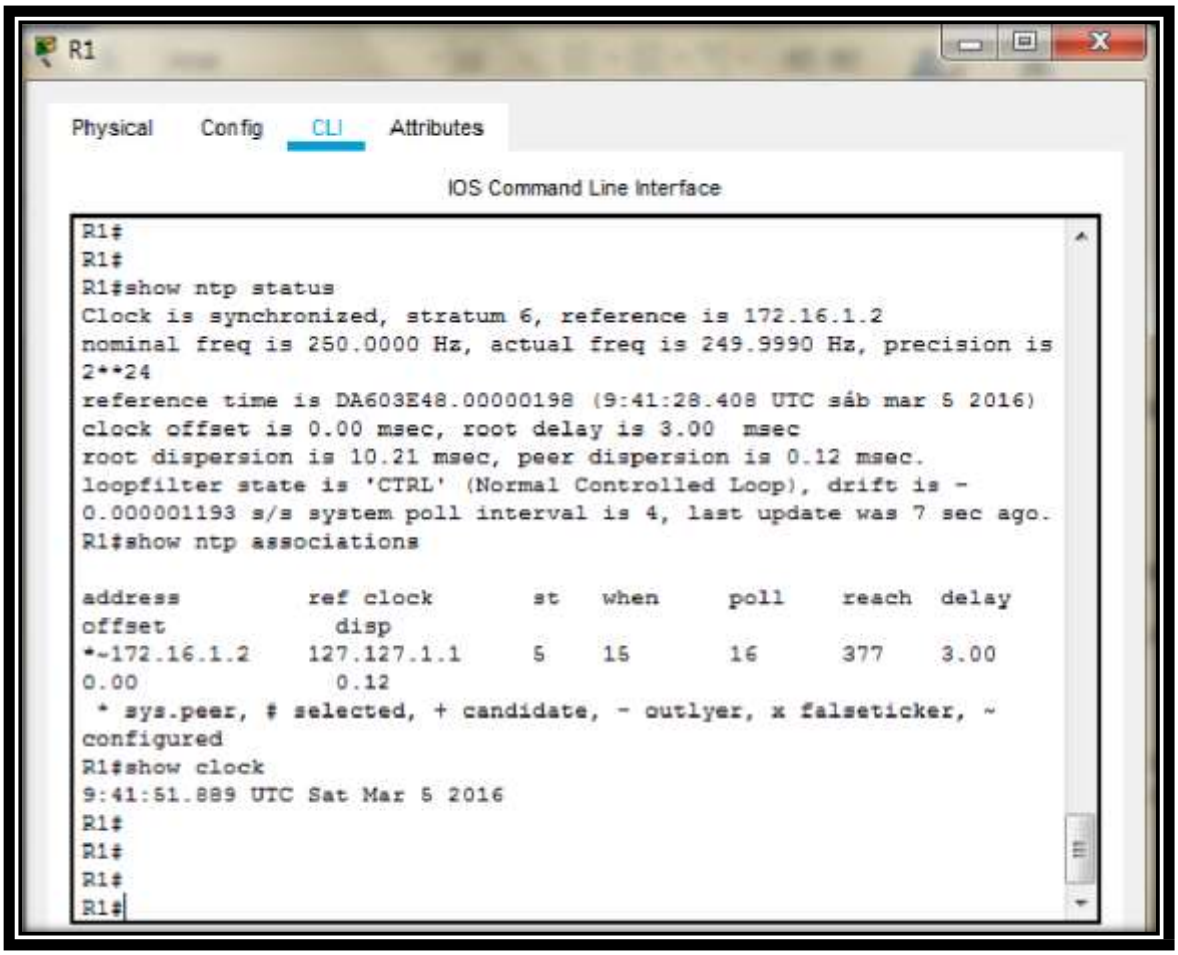

Figura No. 18. Verificación Configuración de NTP en R1

PARTE 7: CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

Paso 20: Restringir el acceso a las líneas VTY en el 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**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Tabla No. 31. Restringir el acceso a las líneas VTY en el R2.

a) Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

  R2> enable
  R2#

- Procedemos a ingresar al modo de configuración.

  R2#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  R2(config)#

- Procedemos a realizar la configuración de la lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2.

  R2(config)#ip access-list standard ADMIN-MGT
  R2(config-std-nacl)#permit host 172.16.1.1
  R2(config-std-nacl)#exit
  R2(config)#

b) Aplicar la ACL con nombre a las líneas VTY

- Procedemos a aplicar la ACL con nombre a las listas VTY

  R2(config)#line vty 0 4
  R2(config-line)#access-class ADMIN-MGT in
  R2(config-line)#exit
  R2(config)#

c) Permitir acceso por Telnet a las líneas de VTY

- Procedemos a realizar el permiso para el acceso por Telnet a las líneas de VTY.

  R2(config)#line vty 0 4
  R2(config-line)#transport input telnet
  R2(config-line)#exit
  R2(config)#

d) Verificar que la ACL funcione como se espera.

- Procedemos a realizar la verificación de acceso Telnet desde R1.

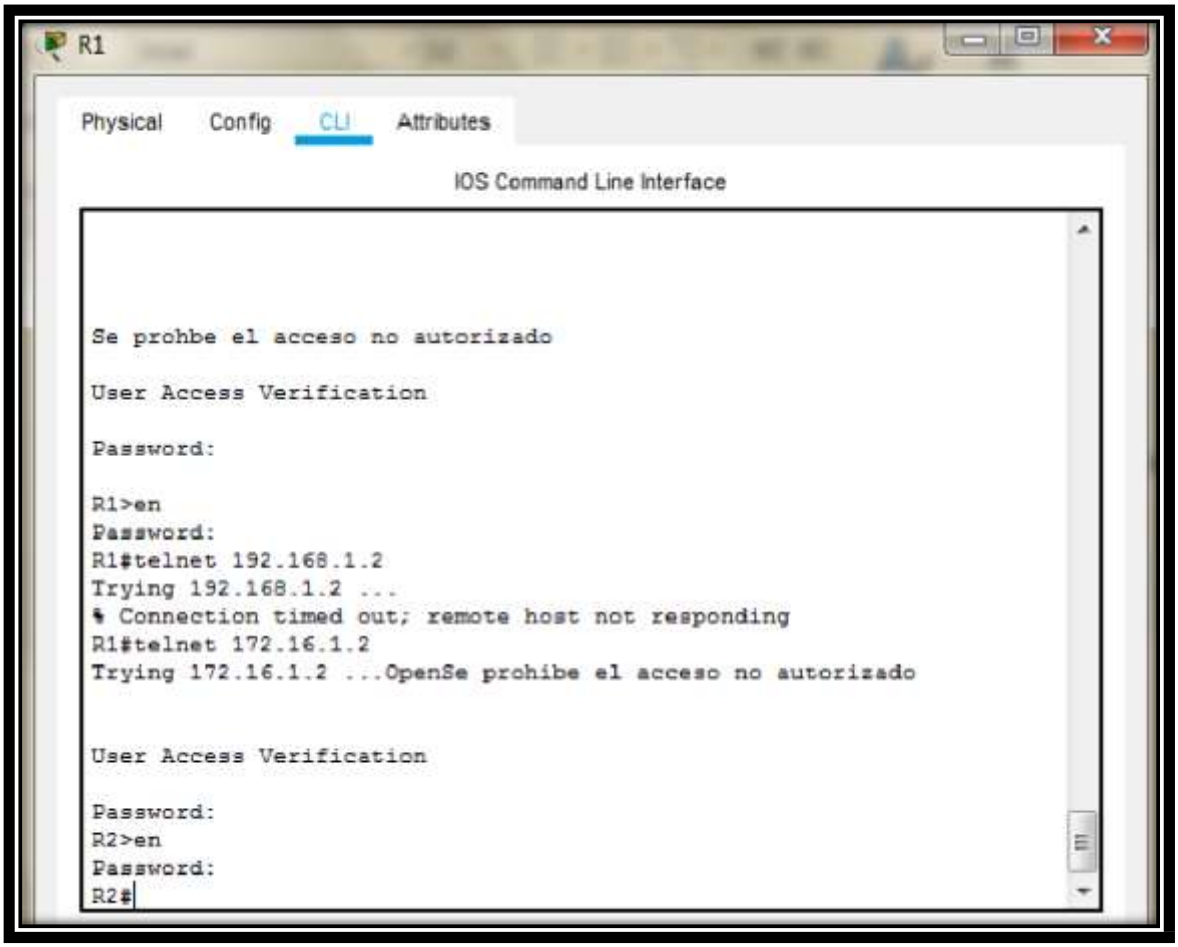

Figura No. 19. Verificación de acceso Telnet desde R1.

- Procedemos a realizar la verificación de acceso Telnet a R2 desde PC-A.

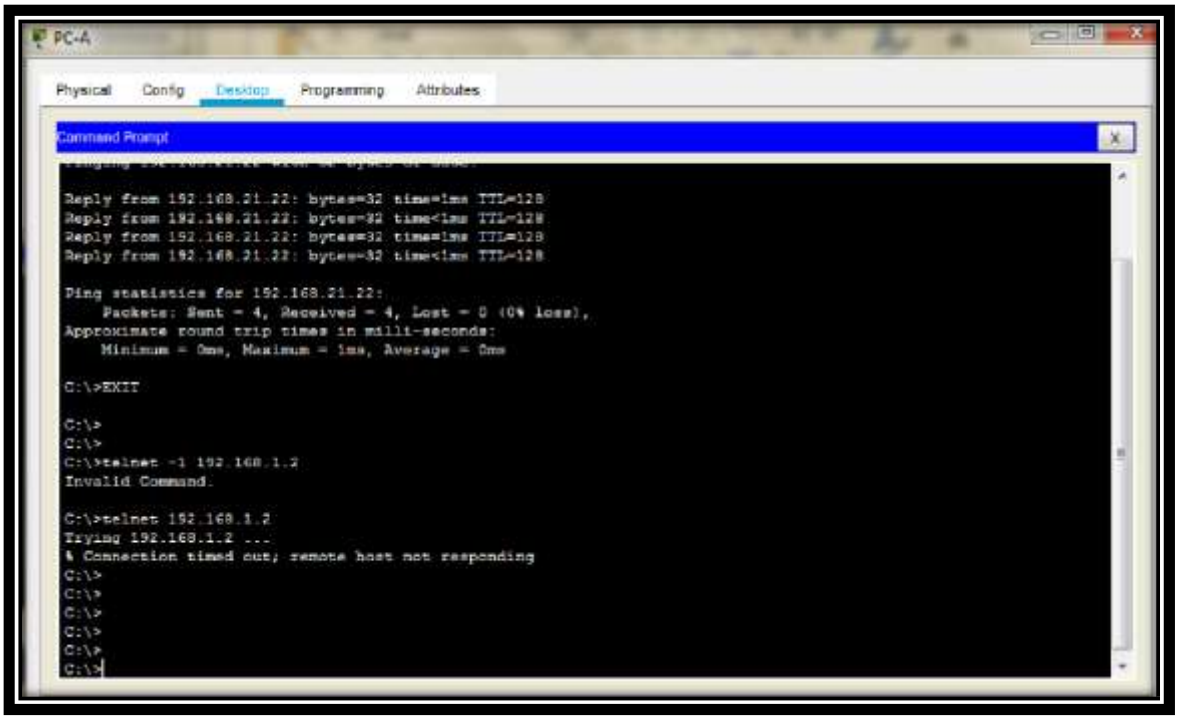

Figura No. 20. Verificación de acceso Telnet a R2 desde PC-A.

Paso 21: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	
Restablecer los contadores de una lista de acceso	
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	
¿Con qué comando se muestran las traducciones NAT?	**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?	

a) Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

- Se accede al Router, seguido a la pestaña CLI
- Presionamos Enter para la iniciación del dispositivo
- Insertamos los comandos IOS para acceder a modo privilegiado.

R2> enable
R2#

- Procedemos a mostrar las coincidencias recibidas por la lista de acceso desde la última vez que se restableció.

R2#show access
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255 (30 match(es))
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.0.255
40 permit 192.168.5.0 0.0.0.255
50 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

R2#

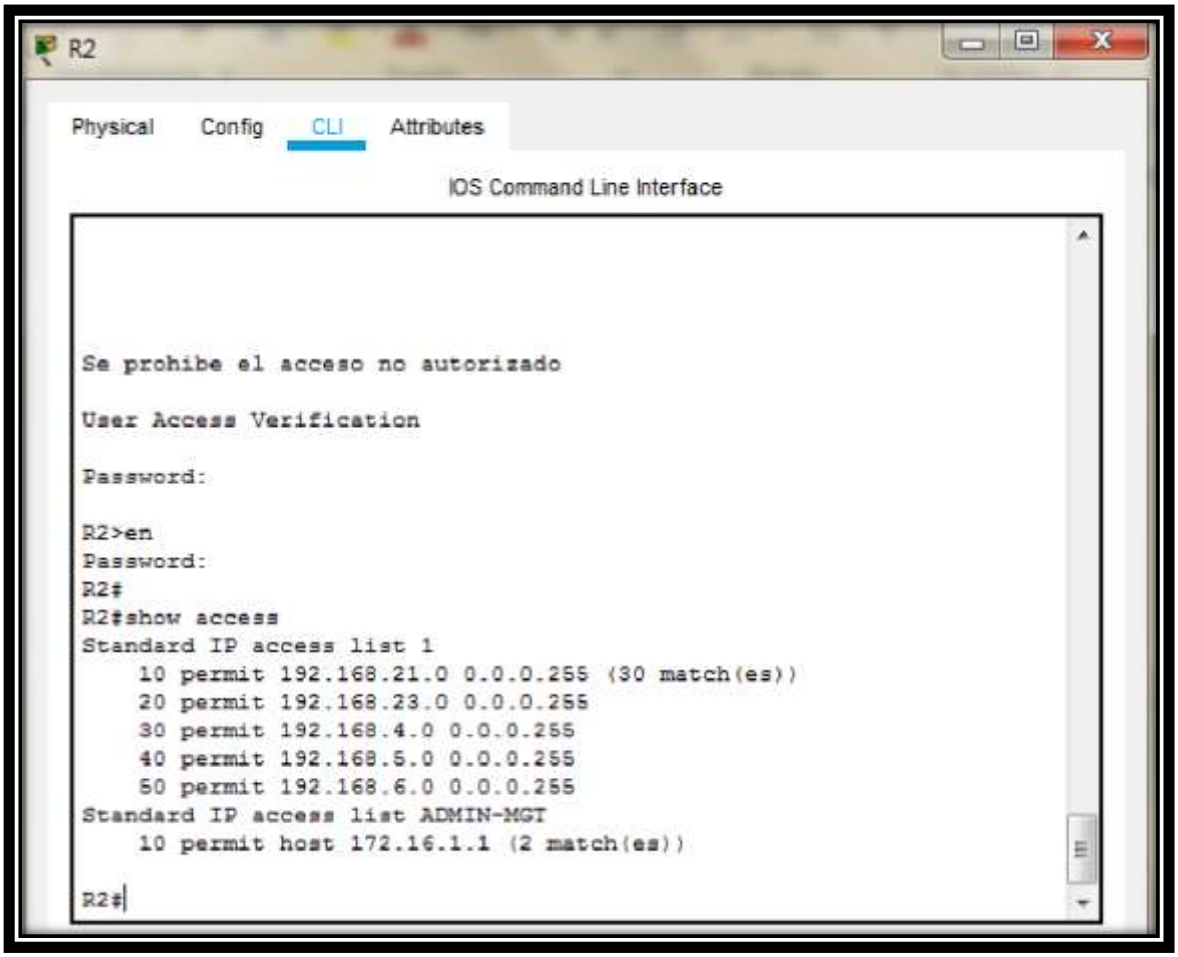

Figura No. 21. Verificación coincidencias recibidas por una lista de acceso desde la última vez que se restableció.

b) Restablecer los contadores de una lista de acceso

- Procedemos a realizar el restablecimiento de los contadores de la lista de acceso.

  R2#clear access-list counters
  R2#

c) ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

- Procedemos a aplicar el comando show ip interface gi0/0 | include Access list, para que nos muestre que ACL se aplica a la interfaz y en qué dirección se aplica.

  R2#show ip interface gi0/0 | include access list
  Outgoing access list is not set
  Inbound access list is not set

R2#show ip interface gi0/0 | include access
Outgoing access list is not set
Inbound access list is not set
IP access violation accounting is disabled
R2#

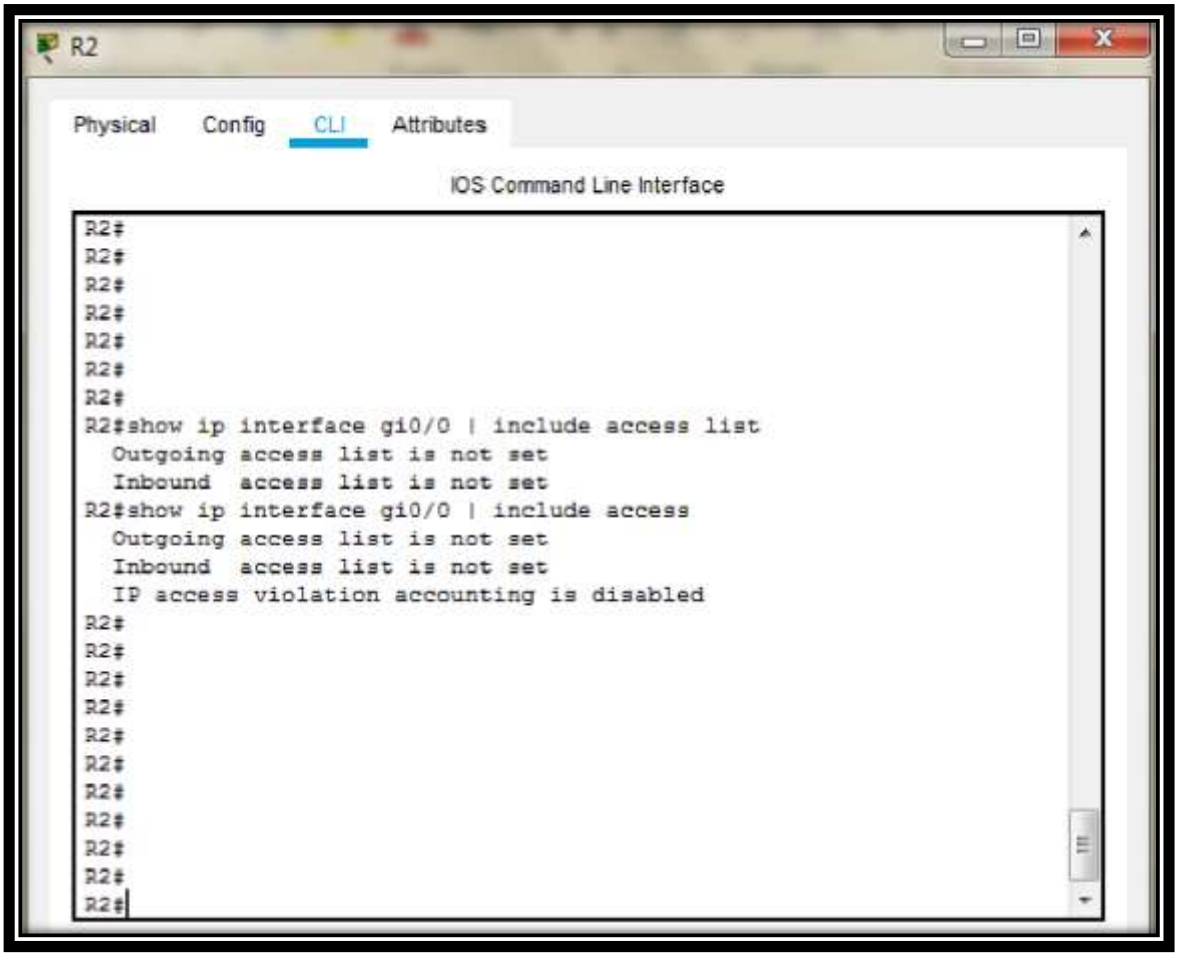

Figura No. 22. Verificación qué ACL se aplica a una interfaz y la dirección en que se aplica.

d) ¿Con qué comando se muestran las traducciones NAT?

- Procedemos a aplicar el Comando show ip nat translations, para que se muestren las traducciones NAT.

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.225:1025192.168.21.21:1025
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1026192.168.21.21:1026
209.165.200.229:80 209.165.200.229:80

tcp 209.165.200.225:1027192.168.21.21:1027
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1028192.168.21.21:1028
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1029192.168.21.21:1029
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1030192.168.21.21:1030
209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.225:1031192.168.21.21:1031
209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.225:1032192.168.21.21:1032
209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.225:1033192.168.21.21:1033
209.165.200.238:80 209.165.200.238:80
tcp 209.165.200.225:1034192.168.21.21:1034
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1035192.168.21.21:1035
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1036192.168.21.21:1036
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.225:1037192.168.21.21:1037 192.168.1.2:23
192.168.1.2:23
tcp 209.165.200.226:1025192.168.21.22:1025
209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.226:1026192.168.21.22:1026
209.165.200.229:80 209.165.200.229:80

R2#

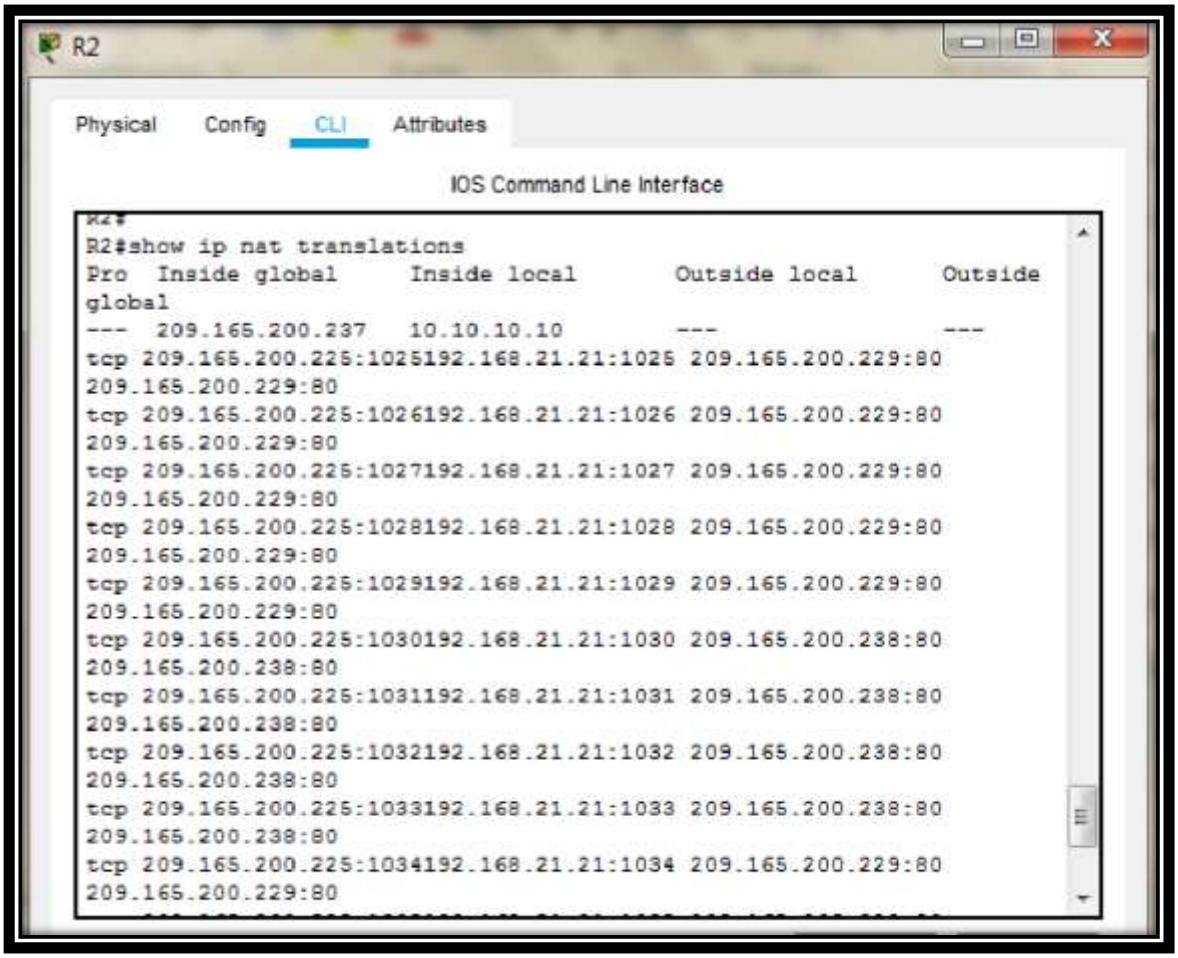

Figura No. 23. Verificación de las traducciones NAT.

e) ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

- Procedemos a aplicar el Comando clear ip nat translation *, para realizar la eliminación de traducciones NAT dinámicas.

  R2#clear ip nat translation *
  R2#

Referencias Bibliográficas

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10