DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRATCIAS CCNP

DEIVIS SMITH MARTINEZ TORRES

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRATCIAS CCNP

DEIVIS SMITH MARTINEZ TORRES

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

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

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Corozal, 15 de mayo 2022

AGRADECIMIENTOS

Primeramente, agradecer a DIOS que me a provisto de vida para llegar a este punto y segundo a mi familia, en especial a mi madre y padre que me han ayudado con los gastos de la universidad y han sido de mi constante apoyo para mi superación académica y personal.

Este es un triunfo que también se debe a los tutores y maestros y a ese incentivo que también aporta la universidad y es la promulgación a la investigación y aprendizaje autónomo, gracias por todo.

CONTENIDO

Pag

LISTA DE TABLAS

Pag.

LISTAS DE FIGURAS

Pag.

GLOSARIO

ACL: Una lista de control de acceso (ACL) de red es una capa de seguridad opcional para su VPC que actúa como firewall para controlar el tráfico entrante y saliente de una o varias subredes.

DHCPv6: Protocolo de configuración dinámica de host para IPv6. DHCPv6 es similar a DHCPv4. Un servidor DHCPv6 asigna dinámicamente información de direccionamiento IPv6 a clientes DHCPv6 al inicio**.**

NAT: La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

NTP: Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

OSPF: es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol, que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

SFTP: SFTP - SSH Protocolo de Transferencia de Archivos Como una extensión al protocolo Shell seguro (SSH), el SFTP se puede utilizar para establecer una sesión segura de transferencia de archivos, en el que el archivo transferido está bloqueado.

SSH: es un protocolo cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VTY: Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un router Cisco varía según el tipo de router y la versión de IOS.

RESUMEN

En este trabajo se presenta el desarrollo de dos escenarios que corresponde al desarrollo de la alternativa de grado diplomado de profundización cisco, donde se proponen dos escenarios con ciertas características y requerimientos especiales que permitan el buen funcionamiento de una red y probada bajo simuladores que permitan ver su comportamiento, así como su respectiva configuración bajo ciertas normas de seguridad que permitan mantener su integridad.

En el primer escenario se construyó una red divida en dos subredes compuestas por un switch, un router y dos hosts, en la que se pide diseñar el esquema de direccionamiento IPV4 para la LAN propuesta, donde los dispositivos de administración de deben proteger con contraseña para evitar el acceso indebido.

Palabras Clave: CISCO, CCNA, Enrutamiento, Redes, Sistemas.

SUMARY

This paper presents the development of two scenarios that corresponds to the development of the cisco deepening diploma degree alternative, where two scenarios are proposed with certain characteristics and special requirements that allow the proper functioning of a network and tested under simulators that allow to see its behavior, as well as its respective configuration under certain security standards that allow its integrity to be maintained.

In the first scenario, a network divided into two subnets composed of a switch, a router and two hosts was built, in which it is requested to design the IPV4 addressing scheme for the proposed LAN, where the management devices must be protected with a password to prevent improper Access.

Keywords: CISCO, CCNA, Routing, Networks, Systems.

INTRODUCCION

En el presente trabajo la directiva del curso propone dos escenarios con característica y requerimientos con el fin de utilizar entornos de simulación que permitan configurar, verificar, y analizar redes de tipo LAN/WAN. Esto con el propósito de analizar su comportamiento, enrutar paquetes y ver el comportamiento de protocolos tales como el TCP, HTTP, entre otros.

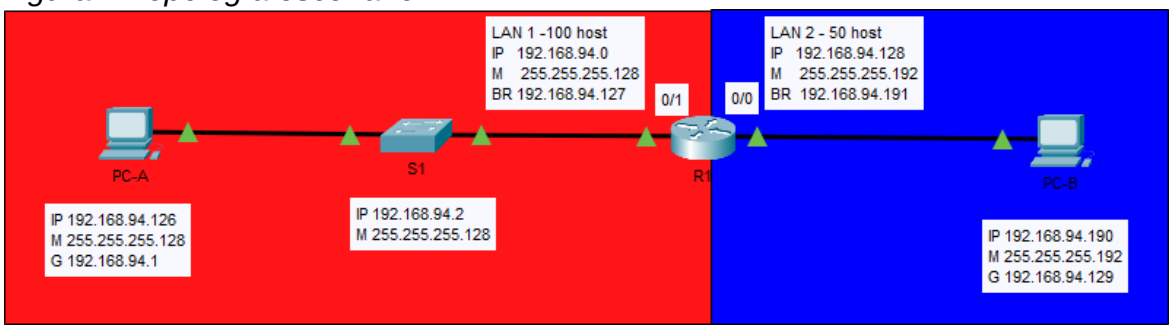
Uno de los objetivos que busca este curso es formar estudiantes capaces y con conocimientos solidos en el desarrollo y construcción de redes LAN/WAN que den solución a un escenario en específico de cierta empresa, entidad, universidad, así como dar solución a problemas eventuales o modificaciones que requiera una mayor expansión de la red.

En el desarrollo del informe final se sustenta que sea estudiado y puesto en práctica los diferentes temas que comprende el curso de CISCO para desarrollar los escenarios presentados en la guía del curso.

DESARROLLO

ESCENARIO 1

Figura 1:Topología escenario 1



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

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

Parte 1: Construya la Red

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

Figura 2 Conexión de la Red

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento. Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1:Tabla de direccionamiento

Ítem	Requerimiento	IP
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.94.0
Requerimiento de host Subred LAN1	100	
Requerimiento de host Subred LAN2	50	
R1 G0/0/1	Primera dirección de host de la subred LAN1	192.168.94.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2	192.168.94.129/26
S1 SVI	Segunda dirección de host de la subred LAN1	192.168.94.2/25
PC-A	Última dirección de host de la subred LAN1	192.168.94.126/25
PC-B	Última dirección de host de la subred LAN2	192.168.94.190/26

Calculando la máscara de una subred

Nuestro primer escenario exige que tengamos 2 subredes, con 150 host, 100 host para la LAN1 y 50 host para la LAN2 por lo tanto necesitamos una máscara de red que nos permita tener 2 subredes y soportar la cantidad de host requerida para cada subred.

Por cuanto nuestra dirección IP es de clase C nuestra mascará de subred tendrá la siguiente forma 255.255.255.128 para la LAN1 y 255.255.255.192 para la LAN2

Creando subredes

LAN 1:

Sabemos que los bits en estado alto “1” en la máscara, especifican la porción de red y que los bits en estado bajo “0” especifican el host en la dirección IP.
Ejemplo si tomamos el primer bit “0” del cuarto octeto desde la izquierda en la máscara y lo transformamos en 1 tendríamos la siguiente mascara
11111111.11111111.11111111.10000000

Sabiendo que los primeros octetos de la máscara representan un 255 en decimal, entonces procedemos a pasar el ultimo octeto que está en binario a decimal.

1*2^7	0*2^6	0*2^5	0*2^4	0*2^3	0*2^2	0*2^1	0*2^0
128	0	0	0	0	0	0	0

Nuestra mascara de subred quedaría de la siguiente manera 255.255.255.128, ahora para saber cuántas subredes admite nuestra mascara, contamos el número de bits en alto que tiene nuestro último octeto, para este caso solo contamos con un bits en estado alto en la parte más alta del byte, por consiguiente 2^1 = 2, cumpliendo con los requerimientos del primer escenario, ahora para saber cuántos host podemos conectar a esa red tomamos el 2 y lo elevamos al número de ceros que contiene el ultimo octeto 2^7 = 128 - 2 = 126, esto debido a que necesitamos una dirección para identificar la red y otra para el dominio de broadcast.

La primera dirección es la que identifica a la red 192.168.94.0 y la dirección de broadcast la conseguimos sumándole 1 al número de host 1 + 126 =127, la dirección de broadcast quedaría como sigue 192.168.94.127.

LAN 2:
Para la LAN 2 solo tenemos una demanda de 50 host por tanto convendría usar una máscara de subred como la siguiente 255.255.255.192 esta nos permitiría conectar hasta 64 -2 = 62 host que es más que suficiente.

1*2^7	1*2^6	0*2^5	0*2^4	0*2^3	0*2^2	0*2^1	0*2^0
128	64	0	0	0	0	0	0

128 + 64 = 192. Ahora para conocer la dirección que identifica la subred LAN2 sumamos 1 más la dirección de broadcast de la primera subred 1 + 127 = 128. Entonces la segunda subred LAN2 la identificaría la siguiente IP 192.168.94.128, y su primera IP seria 192.168.94.129, la dirección de broadcast seria la siguiente 192.168.94.191.

Parte 3: Configure aspectos básicos

Paso1: Configurar los ajustes básicos

Tabla 2:Configuracion Router

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del router R1	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola ciscoenpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas 10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local Nombre usuario: admin Password: admin1pass	R1(config)# username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	1(config)#service passwordencryption
Configure un MOTD Banner	R1(config)#banner motd $Solo personal Autorizado.$
Configurar interfaz G0/0/0	R1(config)#banner motd $Solo personal Autorizado.$ R1(config-if)#description SubRed LAN 2 R1(config-if)#ip address 192.168.94.129 255.255.255.192 R1(config-if)#no shutdown

Configurar interfaz G0/0/1	R1(config)#int g 0/1 R1(config-if)#description SubRed LAN 1 R1(config-if)#ip address 192.168.94.1 255.255.255.128 R1(config-if)#no shutdown
Genera una clave de cifrado RSA - Módulo de 1024 bits	R1(config)#crypto key generate % Incomplete command. R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA keys, keys will be non-exportable...[OK]

Figura 3:Configuración básica de R1

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security passwords min-leght 10
                             ^
% Invalid input detected at '^' marker.

R1(config)#security passwords min-legth 10
                             ^
% Invalid input detected at '^' marker.

R1(config)#security passwords min-length 10
R1(config)# username admin privilege 15 secret adminlpass
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line vty 0 4
```

Tabla 3: Configuración básica del Swith

Ítem	Requerimiento
Desactivar la búsqueda DNS.	S1(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Configure un MOTD Banner	S1(config)#banner motd $Solo personal autorizado$
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024 The name for the keys will be: S1.ccna-lab.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] *Mar 1 7:23:14.439: %SSH-5-ENABLED: SSH 1.99 has been enabled
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.94.2 255.255.255.128 S1(config-if)#no sh
Configuración del gateway	S1(config)#ip default-gateway 192.168.94.1

Figura 4:Configuracion S1, Packet Tracer

```
% Invalid input detected at '^' marker.

Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login exit
                   ^
% Invalid input detected at '^' marker.

S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#banner motd $Solo personal autorizado$
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 7:23:14.439: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.94.2 255.255.255.128
S1(config-if)#no sh
```

Paso 2: Configurar los equipos

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

Figura 5:Configuración del HOST A

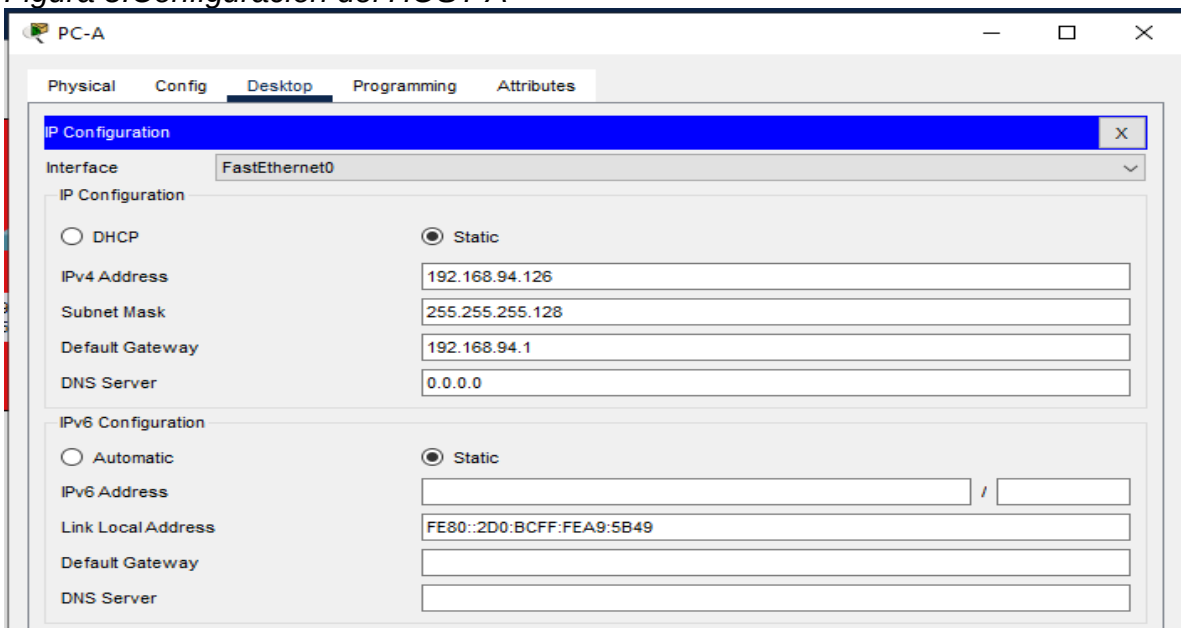


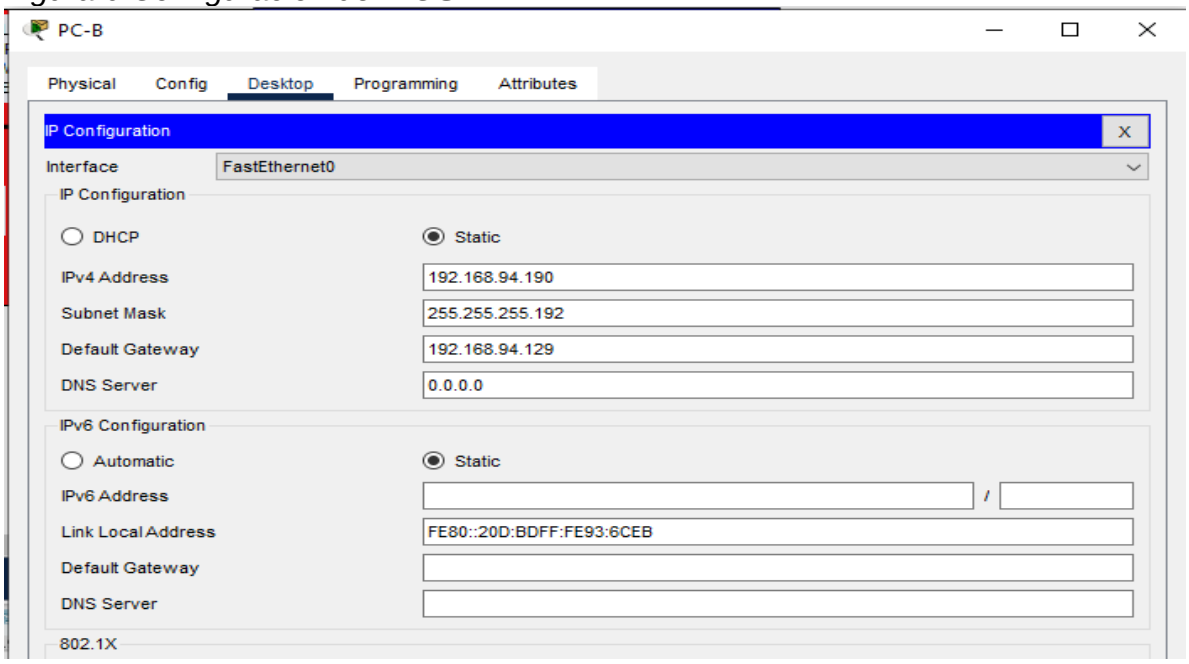
Tabla 4:Configuracion de equipos HOST-A:

PC-A Network Configuration	
Descripción	LAN 1
Dirección física	00D0.D31C.AB09
Dirección IP	192.168.94.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.94.1

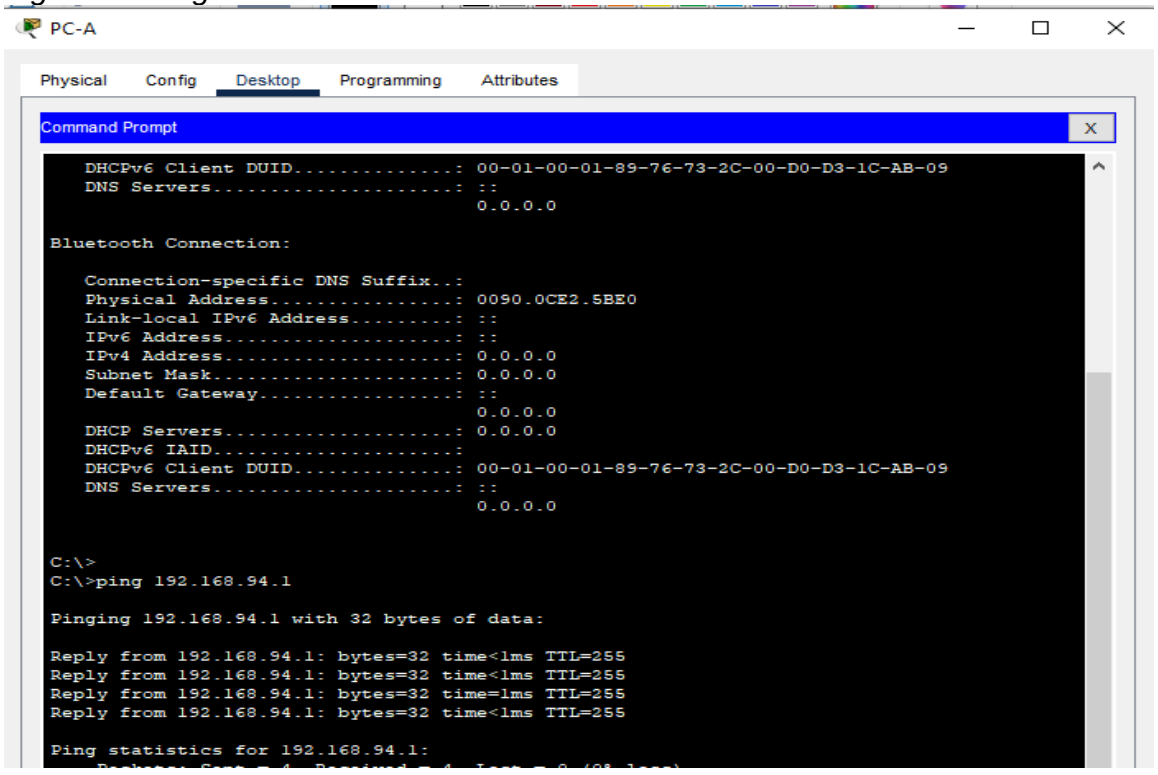
Tabla 5:Configuracion de equipos HOST-B

PC-B Network Configuration	
Descripción	LAN 2
Dirección física	0006.2AE0.E819
Dirección IP	192.168.94.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.94.129

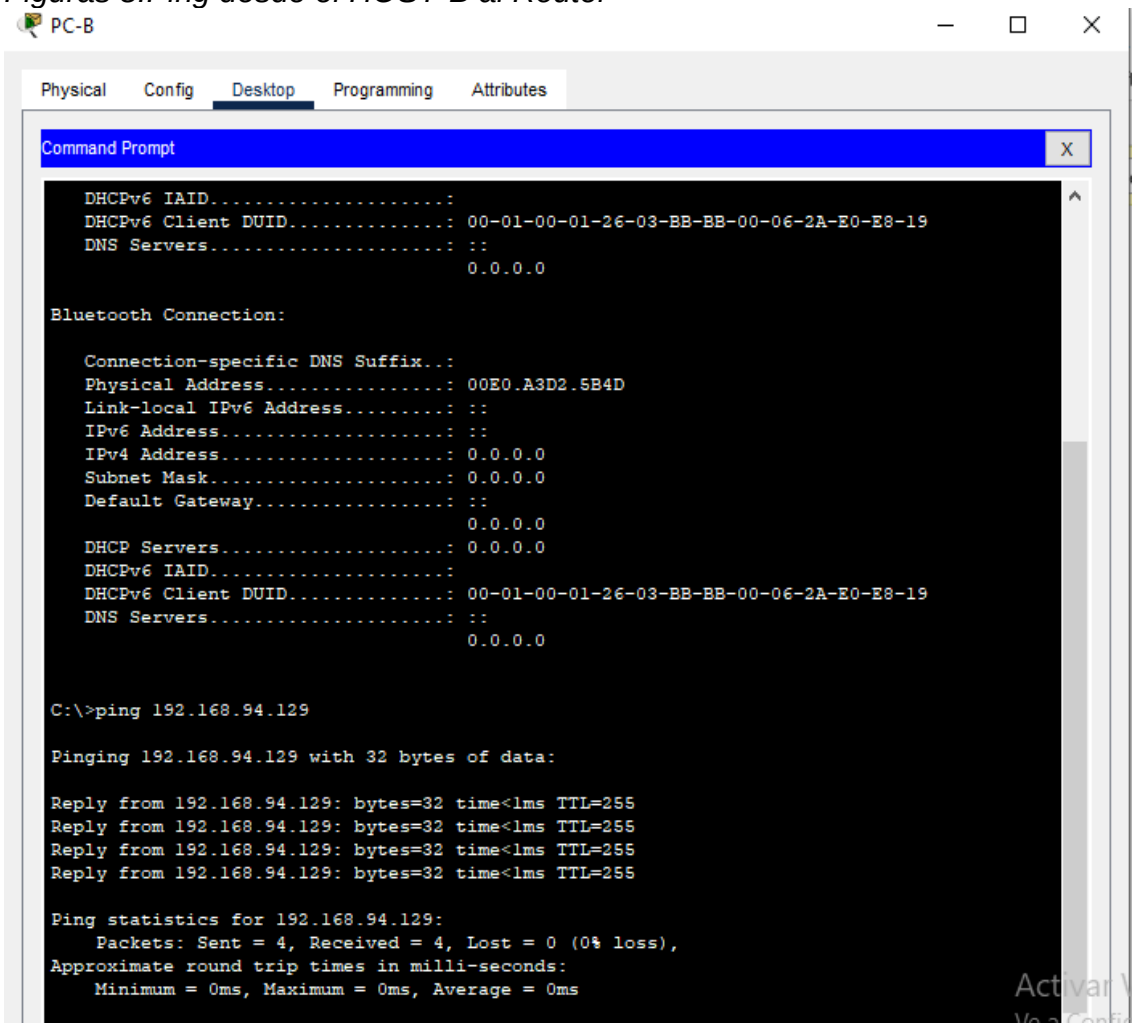
Figura 6:Configuración del HOST B



Figuras 7:Ping desde el HOST-A al Router

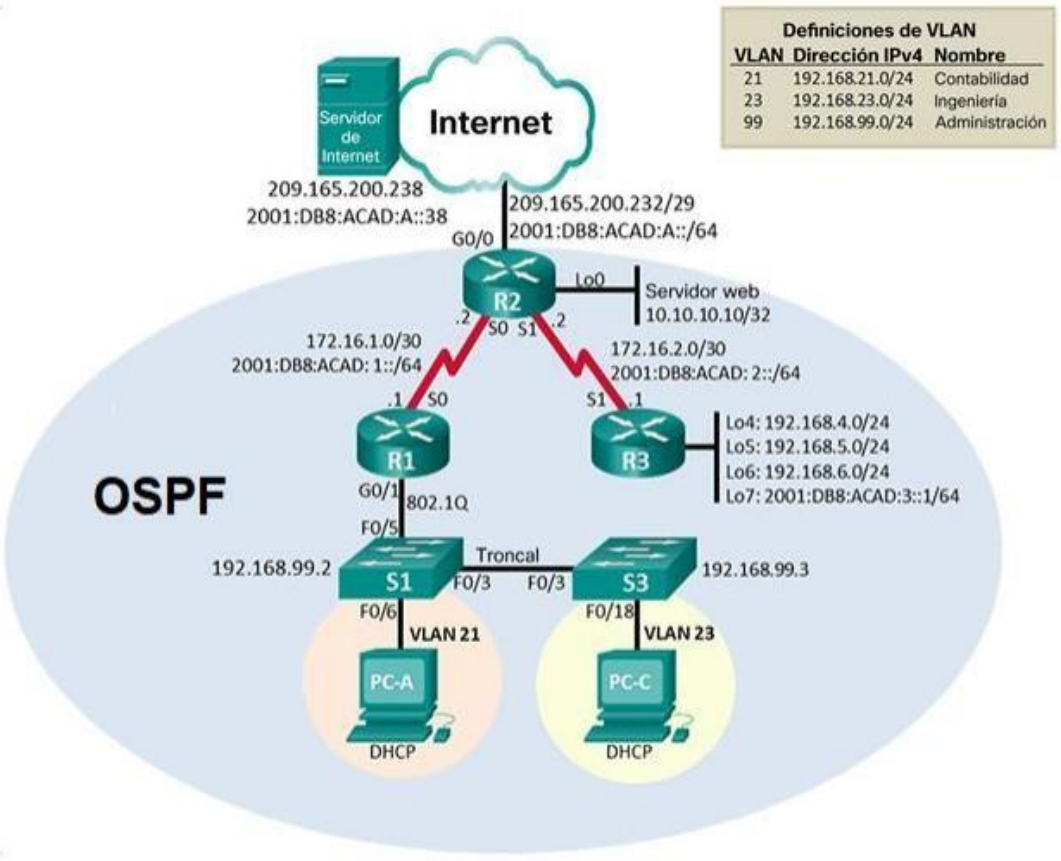


Figuras 8:Ping desde el HOST-B al Router



ESCENARIO 2

Figura 9:Diagrama del Escenario 2



Parte 1: Inicialización de dispositivos.

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6:Reinico de dispositivos

Actividad	Comando de IOS
liminar el archivo startup-config de todos los routers	Router>enable 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
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#enable 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
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free)

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: 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):
Tabla 7:Configuracion de internet

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

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

Paso 2: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8:Configuracion de R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Prohibido el acceso no autorizado$
Interfaz S0/0/0	R1(config)#interface serial 0/0/0 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 12800 Unknown clock rate R1(config-if)#clock rate 128000 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#ipv6 unicast-routing

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9:Configuracion de R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	No soportado

Mensaje MOTD	R2(config)#banner motd $Prohibido el acceso no Autorizado$
Interfaz S0/0/0	R2(config)#interface s0/0/0 R2(config-if)#description conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown R2(config-if)# %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Interfaz S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#description conexion 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 This command applies only to DCE interfaces R2(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	R2(config)#int g 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)#

	%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	R2(config)#interface loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R2(config-if)#description servidor Websimulado R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 giga 0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10:Configuracion de R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado	R3(config)#enable secret class

Contraseña de acceso a la consola cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#
Contraseña de acceso Telnet cisco	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit R3(config)#
Cifrar las contraseñas	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd $Prihibido el Acceso no Autorizado$
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 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)# %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up exit R3(config)#
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)# %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)# %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)# %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)# %LINK-5-CHANGED: Interface Loopback7, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit R3(config)#ipv6 unicast-routing
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

	%Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes actividades:

Tabla 11:Configuracion de S1

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

Paso 6: Configuración del S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12:Configuracion de S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15

	S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Prohibido el Acceso no Autorizado$

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

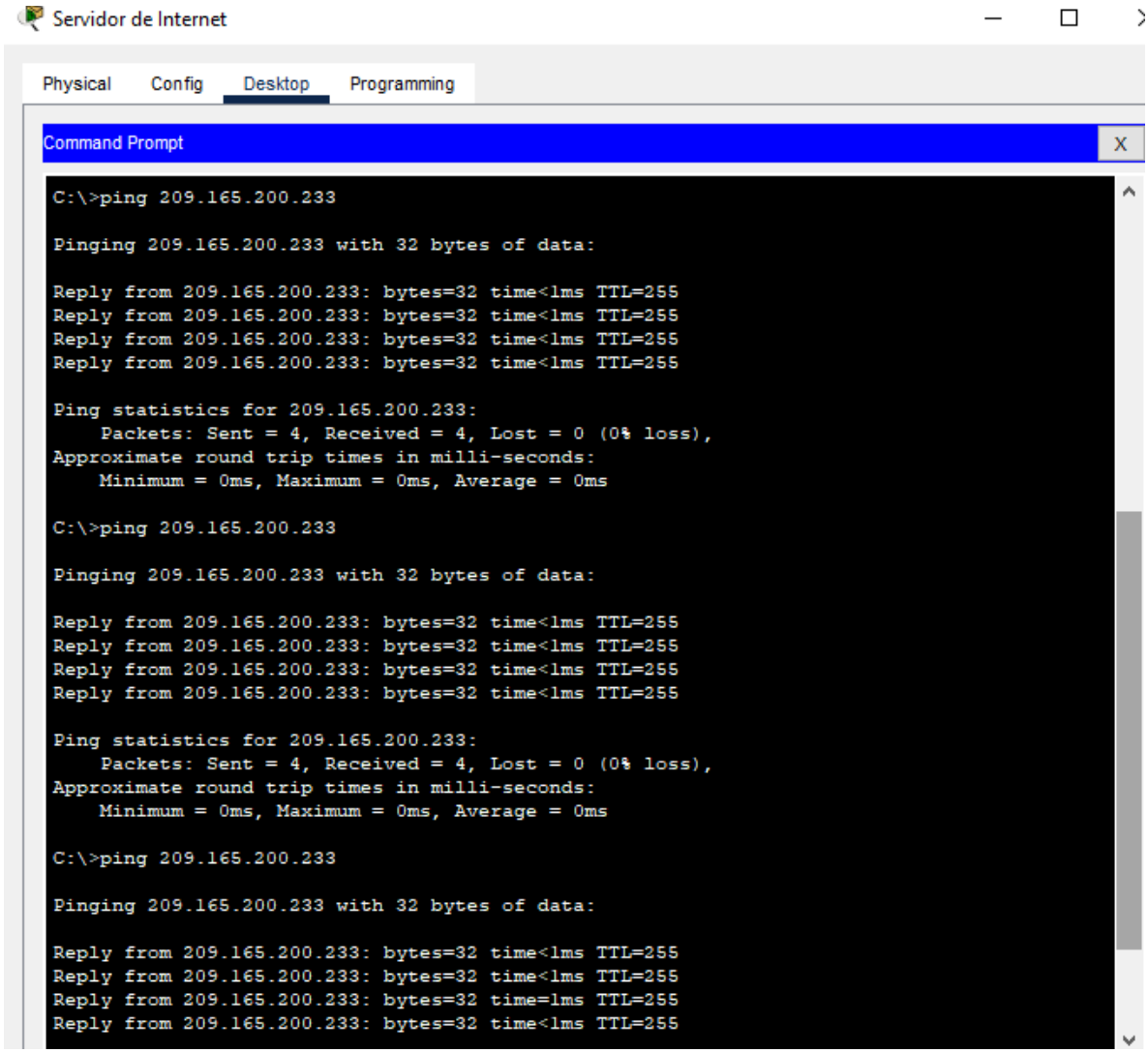
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13:Verificacion de conectividad de RED

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Type escape sequence to abort. 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 1/2/8 ms
R1	R2,S/0/0	2001:db8:acad:1::2	R1#ping 2001:db8:acad:1::2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds: !!!!!

			Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
R2	R3, S0/0/1	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 = 2/7/19 ms
R2	R3, S0/0/1	2001:db8:acad:2::1	R2#ping 2001:db8:acad:2::1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:db8:acad:2::1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Pin exitoso

Figura 10: Pin a Gateway Predeterminado



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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14:Configuracion de seguridad del switch

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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
Asignar la dirección IP de 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
Asignar el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f 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
Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface f 0/5 S1(config-if)#swichport mode trunk S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos 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
Asignar F0/6 a la VLAN 21	S1(config)#interface range f0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15:Configuracion de vlan S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name C S3(config-vlan)#no name C 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
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchpor mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit

Configurar el resto de los puertos como puertos de acceso	S3(config)#interface range fa0/1-2, fa0/4, fa0/6-24 S3(config-if-range)#switchport mode access S3(config-if-range)#exit
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2,f0/4,f0/7-17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16:Configuracion dot1q en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g 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
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/1.23 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
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.23 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
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17:Verificacion de conexion

DESDE	A	DIRECCION IP	RESULTADOS DE PING
S1	R1,dirección VLAN 99	192.168.99.1	Type escape sequence to abort. 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 = 0/0/0 ms
S3	R1,dirección VLAN 99	192.168.99.1	Type escape sequence to abort. 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 = 0/0/0 ms
S1	R1,dirección VLAN 21	192.168.21.1	Type escape sequence to abort. 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	Type escape sequence to abort. 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 = 0/0/0 ms

Figura 11: Pin en S1 ala vlan 99

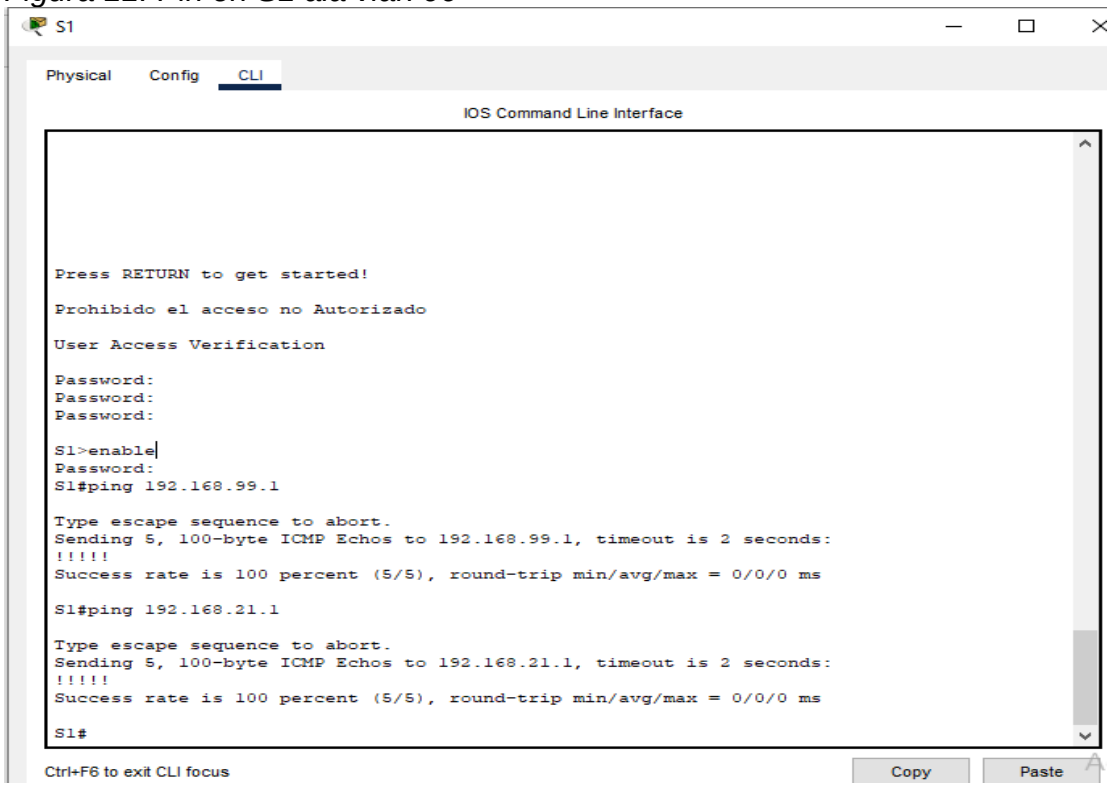
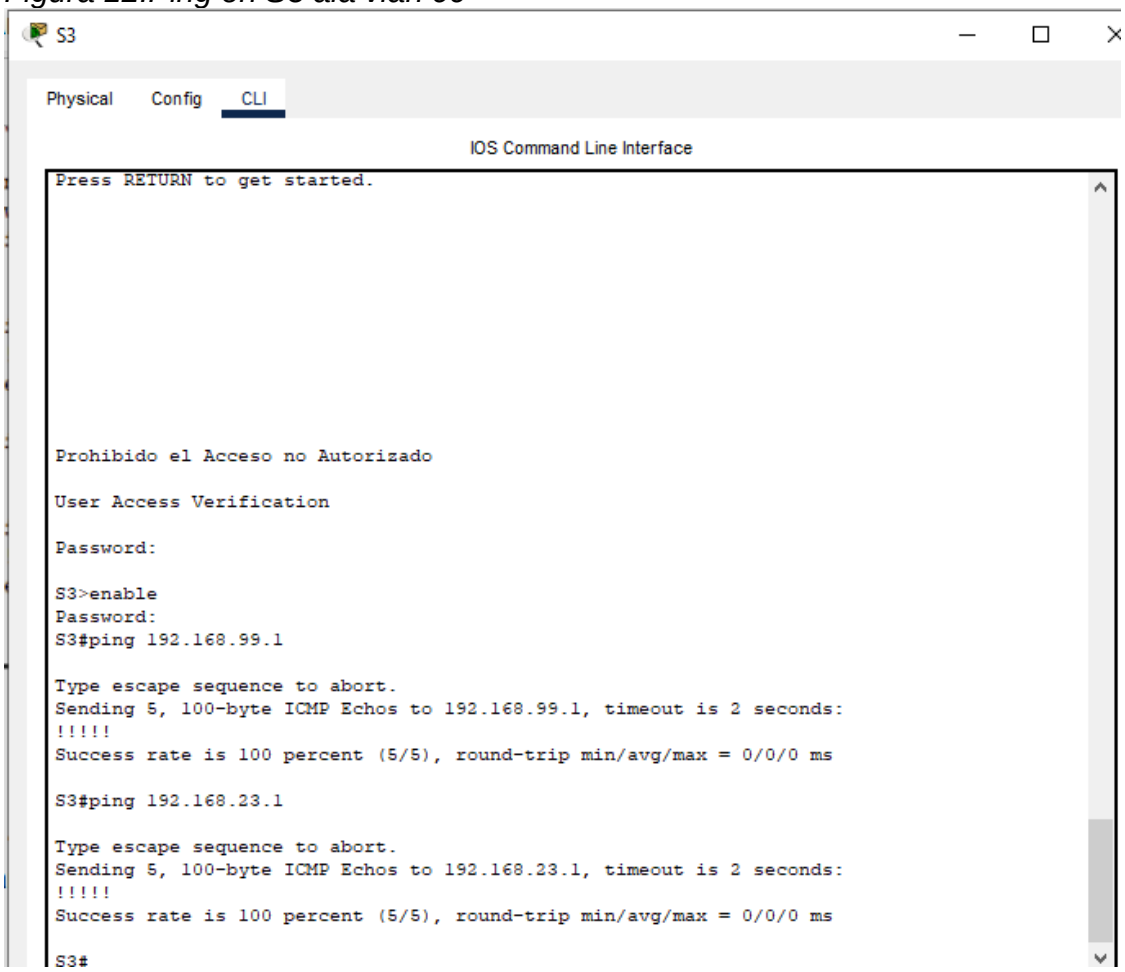


Figura 12:Ping en S3 ala vlan 99



Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18:Configuracion OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0

	R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface gi0/1.21 R1(config-router)#passive-interface gi0/1.23 R1(config-router)#passive-interface gi0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-sumary

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19:Configuracion OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive- interface lo0
Desactive la sumarización automática.	Aplica solo para RIP

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20:Configuracion OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router osp 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
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

Desactive la sumarización automática.	Aplica solo para RIP

Paso 4: Verificar la información de OSPF

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

Tabla 21:Verificación protocolo OSPF

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

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22:Configuracion de R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	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
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

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23:Configuracion NAT en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No soportado
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una 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

Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 24:Verificacion DHCP Y NAT

Prueba
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
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

Figura 13:IP PCA con DHCP

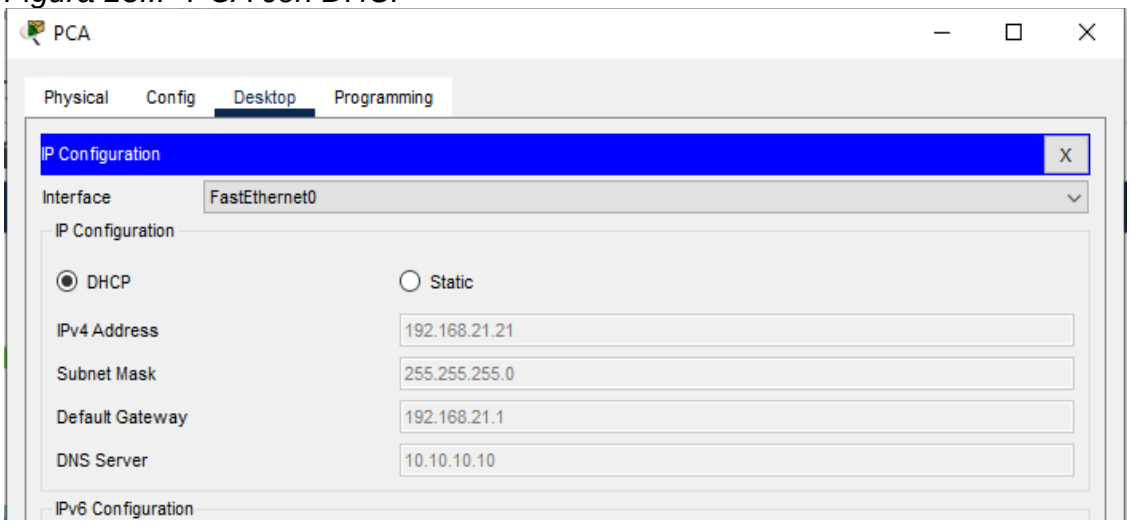


Figura 14:IP de PCC con DHCP

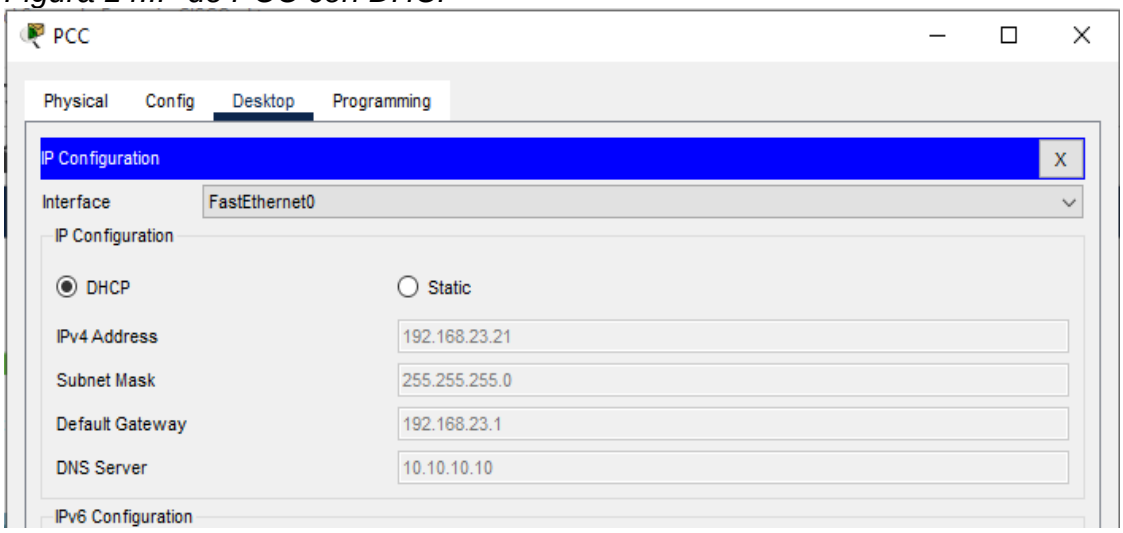


Figura 15:Pin des PCA a PCC

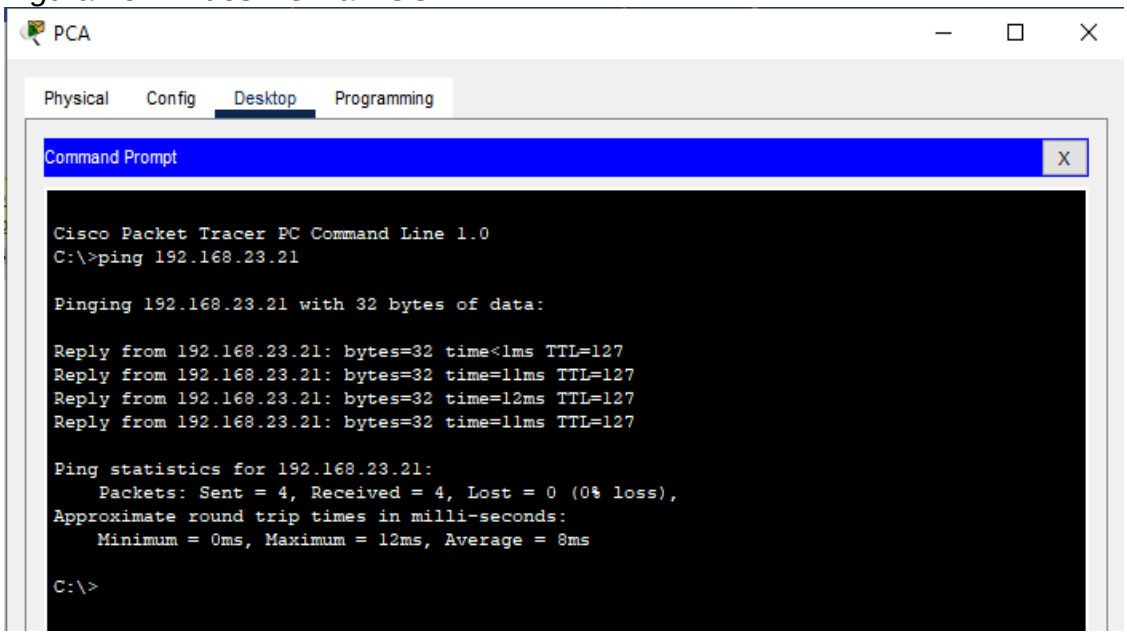


Figura 16:Ping desde PCC a PCA

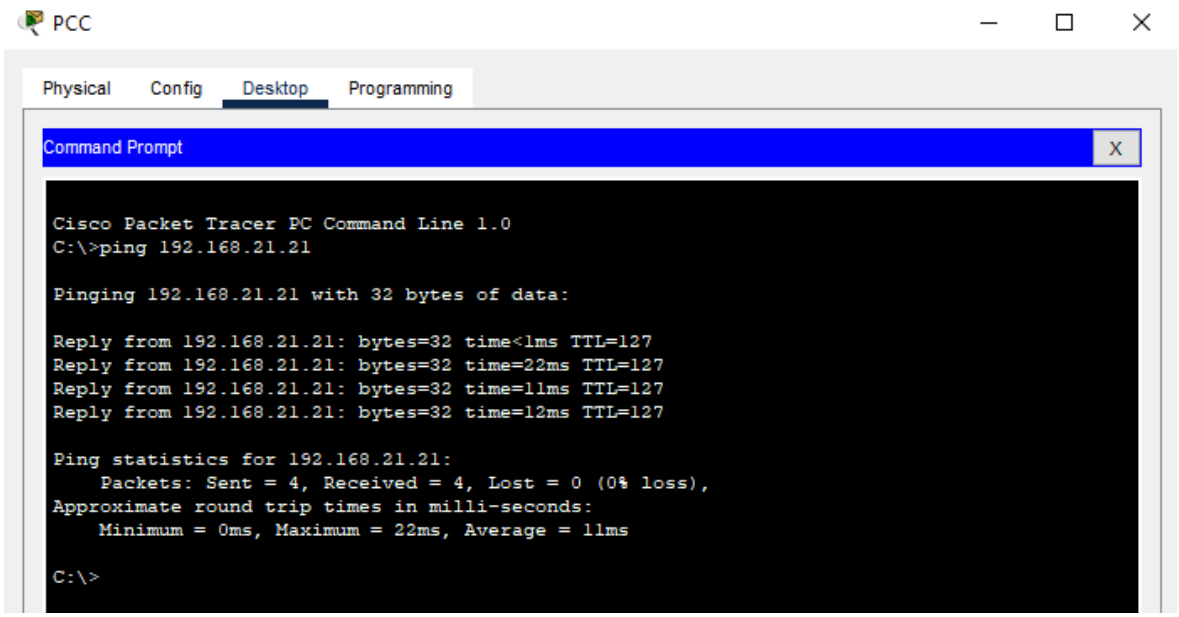
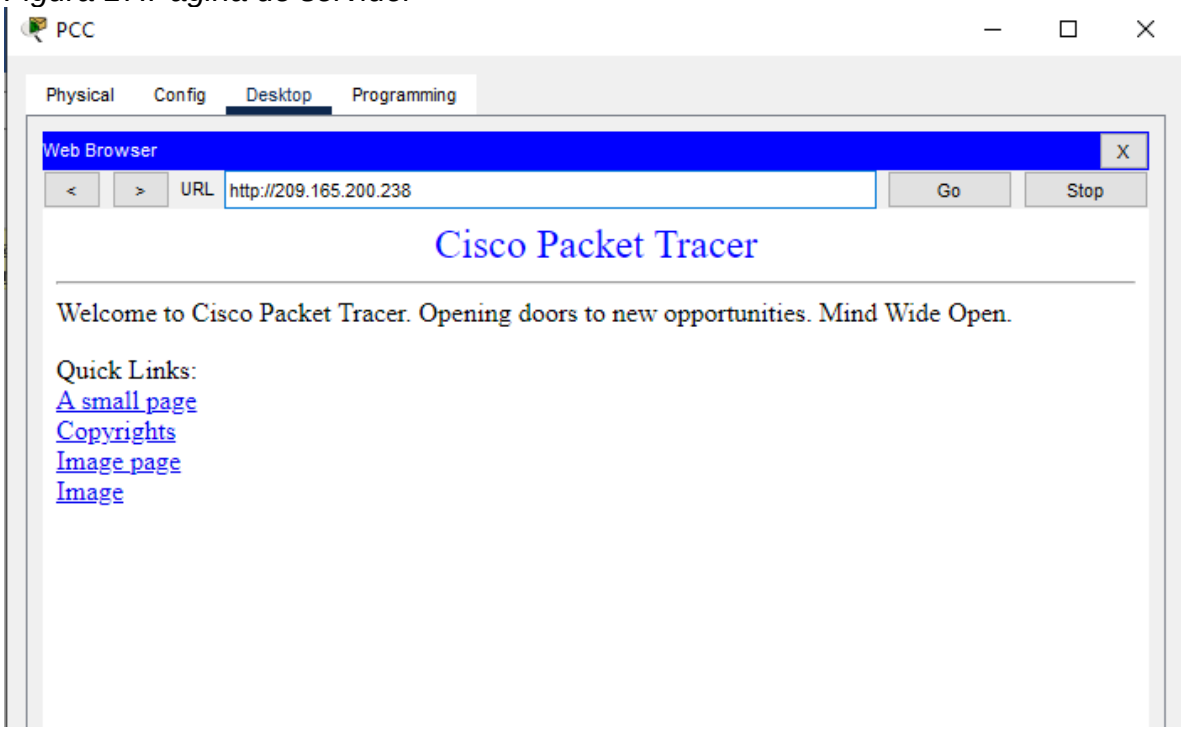


Figura 17:Pagina de servidor

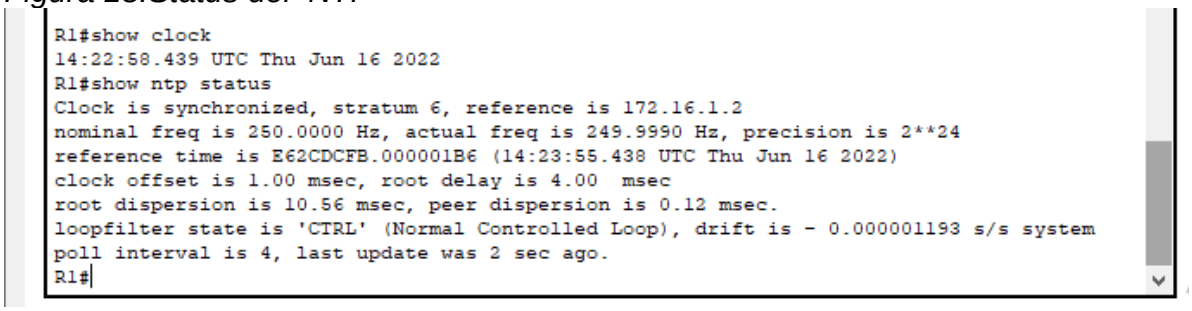


Parte 6: Configurar NTP

Tabla 25:Configuracion NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 14:06 16 jun 2022
Configure R2 como un maestro NTP	R2(config)#ntp master 5
Configurar R1 como un cliente NTP	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	

Figura 18:Status del NTP



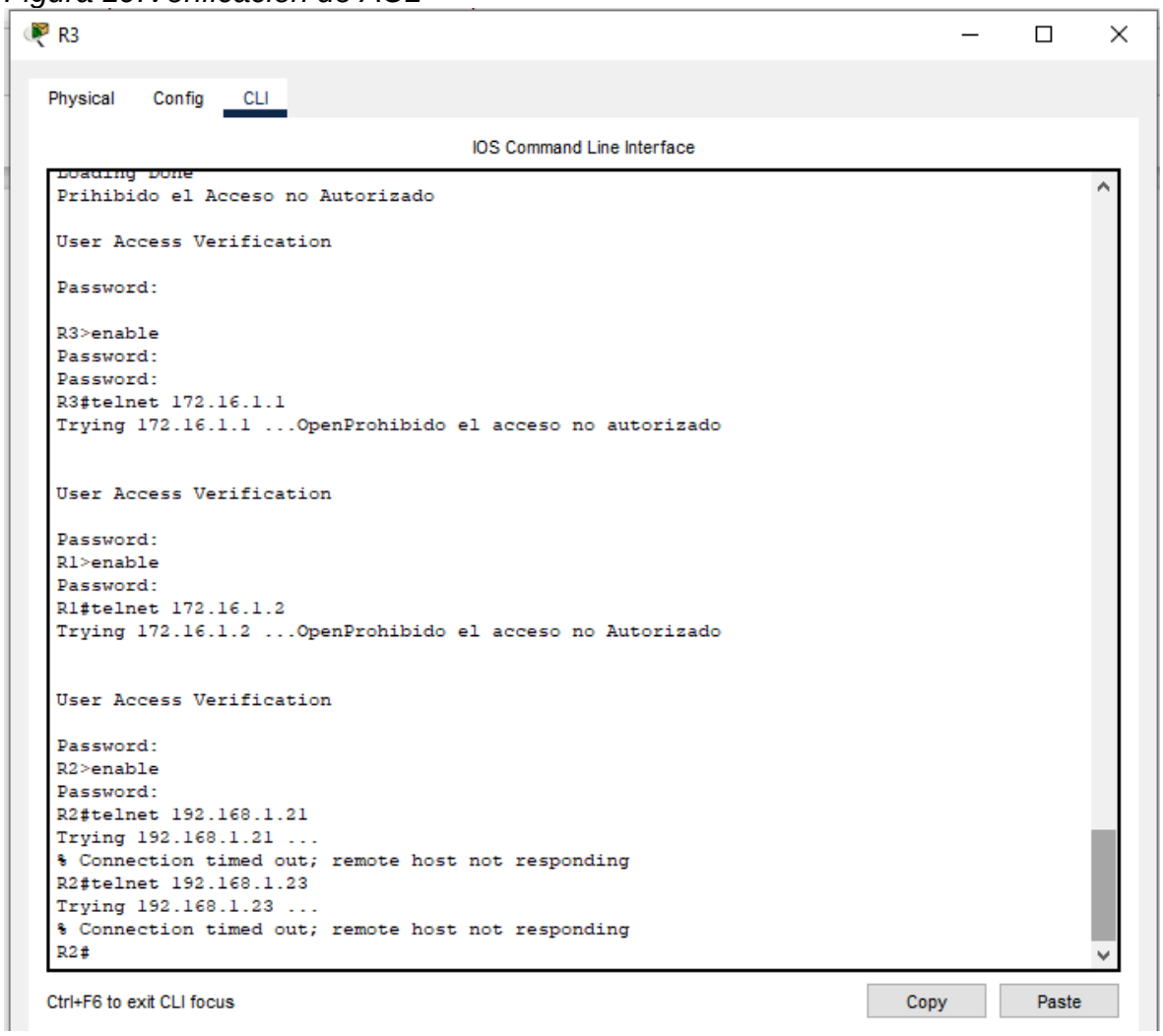
Parte 7. Configurar y verificar las listas de control de acceso ACL)

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

Tabla 26:Configuracion del control de acceso ACL

Elemento o tarea de configuración	Especificación
Configurar una 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
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	

Figura 19:Verificacion de ACL



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

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

Tabla 27:Listas de acceso desde la ultima vez de ingreso

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1#show access-list

Restablecer los contadores de una lista de acceso	R1#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1 (config)#interface Fa0/1 R1 (config-if)#ip access-group 1 out
¿Con qué comando se muestran las traducciones NAT?	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?	R1(config)#clear ip nat translation

CONCLUCIONES

El diplomado de profundización cisco permite validar la capacidad de planificar, verificar e implementar y dar soluciones a redes de tipo empresarial LAN/WAN, mediante entornos de simulación como Pakect Tracer, GNS3, que nos permitan tener un análisis de su funcionamiento y requerimientos antes de llevarlos a la parte física con el fin de tomar la mejor ruta más corta y menos costosa que nos permita ejecutar el proyecto de red.

Es importante establecer niveles de seguridad básicos, que permitan proteger los dispositivos para su acceso a usuarios no autorizados que se encuentren físicamente frente a los dispositivos, así como también a usurarios remotos mediante contraseñas con cifrado SSH e encriptada tanto para las líneas de consola, así como las VTY.

Los conocimientos alcanzados en el curso, serán necesarios para el desarrollo de redes escalables mediante jerarquía que permita el mayor rendimiento óptimo de la red y que permita una mayor expansión de la red sin interrumpir el funcionamiento del servicio de internet en caso de que se requiera.

En el escenario 2 se empleó el protocolo de routing estático RIP o dinámico OSPF, así como configurar esquemas de conmutación, mediante el uso de protocolos basados en STP y VLANS, proporcionar conectividad, seguridad y acceso ala WAN mediante el uso de protocolo DHCP y traducciones de direcciones IP con NAT.

El curso ofrece una cobertura integral y completa sobre temas de redes, incluidos: principios básicos de enrutamiento y conmutación IP, seguridad y servicios de red, y programabilidad y automatización de la red; a la vez que brinda a mi carrera profesional numerosas oportunidades de experiencia práctica y desarrollo de destrezas profesionales que permita construir redes fiables y seguras.

BIBLIOGRAFIA

BORONAT SEGUI, Fernando. Configuración DHCP en routers CISCO. 2015.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento%20IP.pdf

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter9_Divisi%c3%b3n%20de%20redes%20IP%20en%20subredes.pdf

CISCO. (2019). Capa de transporte. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter7_Capa%20de%20transporte.pdf

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter10_Capa%20de%20aplicacion.pdf

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter11_Es%20una%20red.pdf

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/03_Dynamic_Routing.pdf

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/04_Switched_Networks.pdf

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. http://vapenik.s.cnl.sk/pcsiete/CCNA2/09_NAT_for_IPv4.pdf