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

JOHANA MARCELA BENAVIDEZ VALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
CALI - COLOMBIA
2021

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

JOHANA MARCELA BENAVIDEZ VALENCIA

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

DIRECTOR:
MSc. MARIA ALEJANDRA LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
CALI, COLOMBIA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cali, Colombia, 17 de octubre de 2021

AGRADECIMIENTOS

Expreso total agradecimiento a cada uno de los tutores que, con su retroalimentación, ánimo y dedicación aportaron en mi proceso de formación, especialmente en el desarrollo del diplomado que como opción de grado me sitúa muy cerca de cumplir con el objetivo de culminar la ingeniería en sistemas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

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.

IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o que corresponde al nivel de red del modelo TCP/IP.

Router: dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Subred: es un rango de direcciones lógicas.

Switch: 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).

RESUMEN

En el presente informe se desarrollará la prueba de habilidad planteada por la academia CISCO para el diplomado de profundización CCNA en la cual se requiere la implementación de dos redes simuladas en la herramienta packet tracer, inicialmente se realizará la instalación, cableado y enrutamiento de los componentes requeridos, tales como: router, switch y equipos de cómputo, todo con las buenas prácticas de seguridad sugeridas.

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

ABSTRACT

In this report, the skill test proposed by the CISCO academy for the CCNA deepening diploma will be developed, which requires the implementation of two simulated networks in the packet tracer tool, initially the installation, wiring and routing of the components will be carried out. required, such as: router, switch and computer equipment, all with suggested good security practices.

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

INTRODUCCIÓN

Dentro del proceso de aprendizaje que se brinda en el diplomado de profundización CCNA de la academia CISCO, identificamos que como objetivos principales se encuentra el poder apropiar conceptos básicos y propios de la administración de redes domésticas y corporativas, es por esto que en este componente práctico y apoyados con la herramienta packet tracer se realizará el montaje de una red compuesta por un Router, un Switch y dos equipos de cómputo, en el que se deberá garantizar configuración adecuada, protocolos de seguridad informática aplicada y lo más importantes conectividad y comunicación de cada uno de su componentes.

Como componente práctico dos se encuentra un modelo de red más avanzada en la que se incluirá configuración de routing dinámico OSPF, asignación de direccionamiento dinámico DCHP, traducción de redes NAT y listas de control de acceso, entre otros; todo lo mencionado con la aplicación de buenas prácticas de seguridad que permitan tener conectadas las redes internas y externas de manera adecuada.

ESCENARIO 1

En este 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.

Topología.

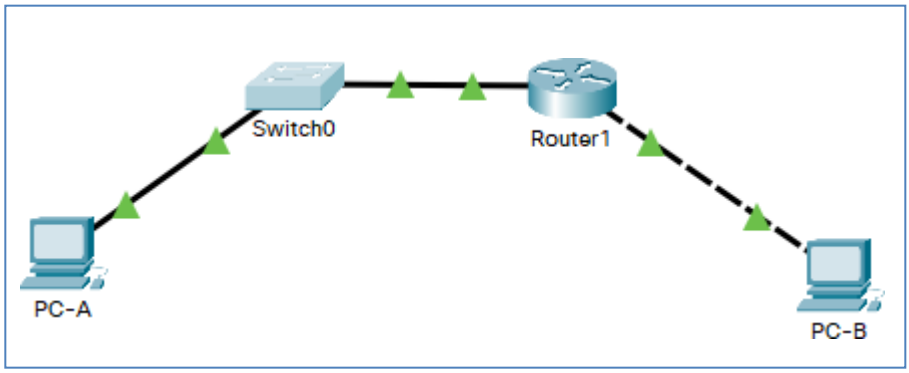
Ilustración 1 Topología

Fuente: Elaboración propia.

Construcción de Red.

Detalle de la red diseñada en herramienta Packet tracer

Ilustración 2 Construcción de red



Fuente: Elaboración propia.

Esquema de direccionamiento

Teniendo en cuenta el digito de documento, trabajaremos con el segmento 192.168.49.0, mascara 25

Tabla 1 Esquema de direccionamiento

Subred	Dirección IP	Mascara	Intervalo	Broadcast
1	192.168.49.0	255.255.255.128/25	192.168.49.1 192.168.49.126	192.168.49.127
2	192.168.49.128	255.255.255.128/25	192.168.49.129 192.168.49.254	192.168.49.255

Tabla 2. Requerimientos Direccionamiento

Ítem	Requerimiento
Direccionamiento de Red	192.168.49.0
Requerimiento de host subred LAN1	100
Requerimiento de host subred LAN2	50
R1 G0/0/1	192.168.49.1
R1 G0/0/0	192.168.49.129
S1 SV1	192.168.49.2
PC-A	192.168.49.126
PC-B	192.168.49.254

Paso 1: Configurar ajustes básicos

Configuración de Router 1 mediante comandos de consola (CLI)

Tabla 3. Configuración R1

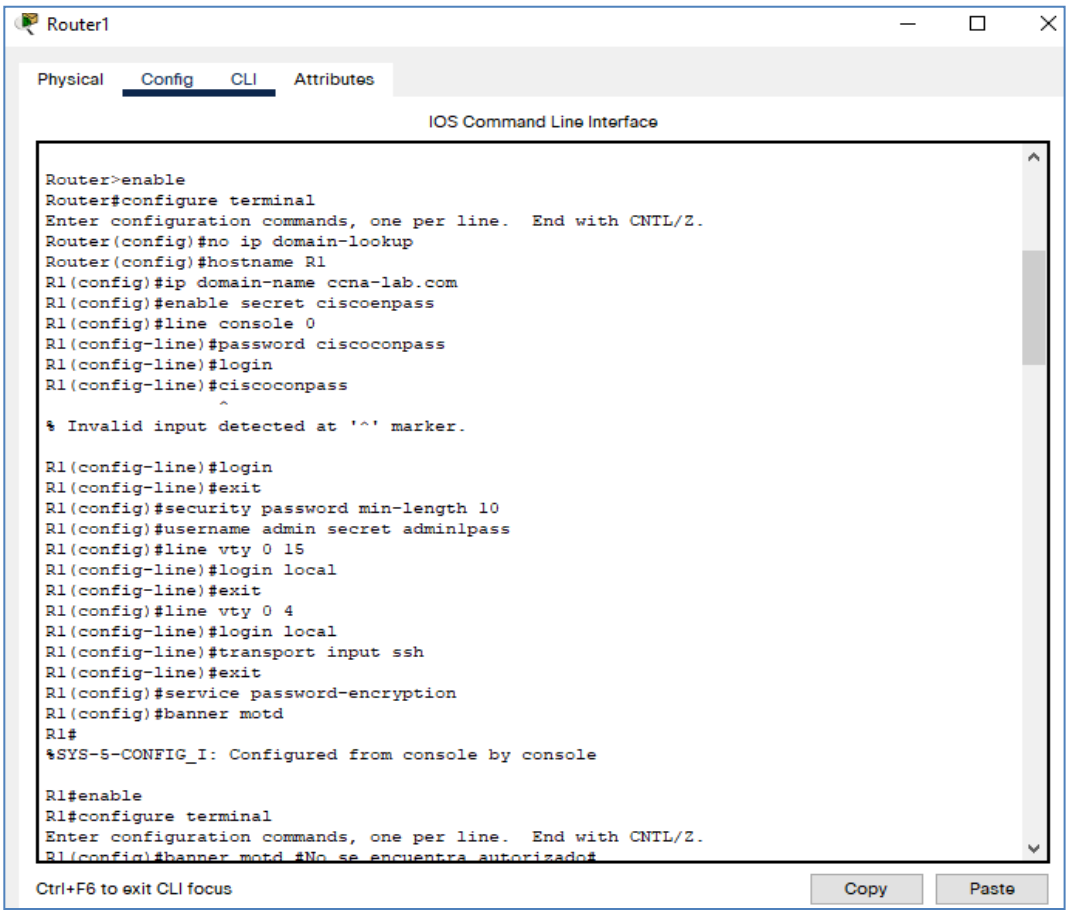
Configuración R1.	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS Nombre del router R1	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#hostname R1
Nombre de dominio ccna-lab.com	R1(config)#ip domain-name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#ciscoconpass
Establecer la longitud mínima para las contraseñas 10 caracteres	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local *Nombre de usuario: admin Password: admin1pass*	R1(config)#username admin 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 4 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #No se encuentra autorizado#
Configurar interfaz G0/0/0	R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 192.168.49.1 255.255.255.128 R1(config-subif)#description bikes R1(config-subif)#no shutdown R1(config-subif)#exit
Configurar interfaz G0/0/1	R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 192.168.49.129 255.255.255.128 R1(config-subif)#description trikes R1(config-subif)#no shutdown R1(config-subif)#exit
Generar una clave de cifrado RSA	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)#exit

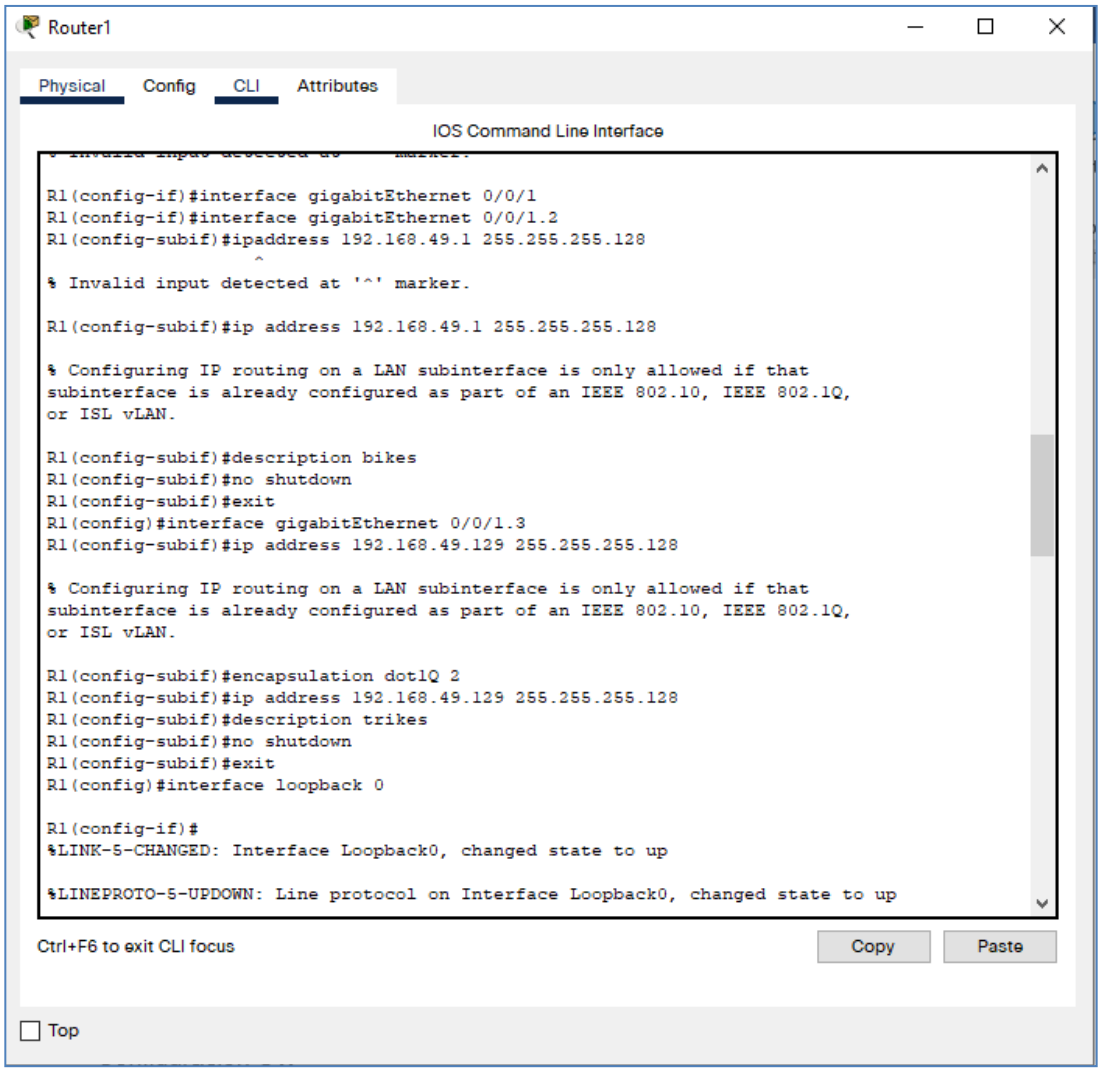
Ilustraciones de configuración aplicada Router R1.

Ilustración 3. Configuración R1



Fuente: Elaboración propia.

Ilustración 4. Configuración R1 adicional



Fuente: Elaboración propia.

Configuración de Switch 1 mediante comandos de consola (CLI)

Tabla 4. Configuración S1

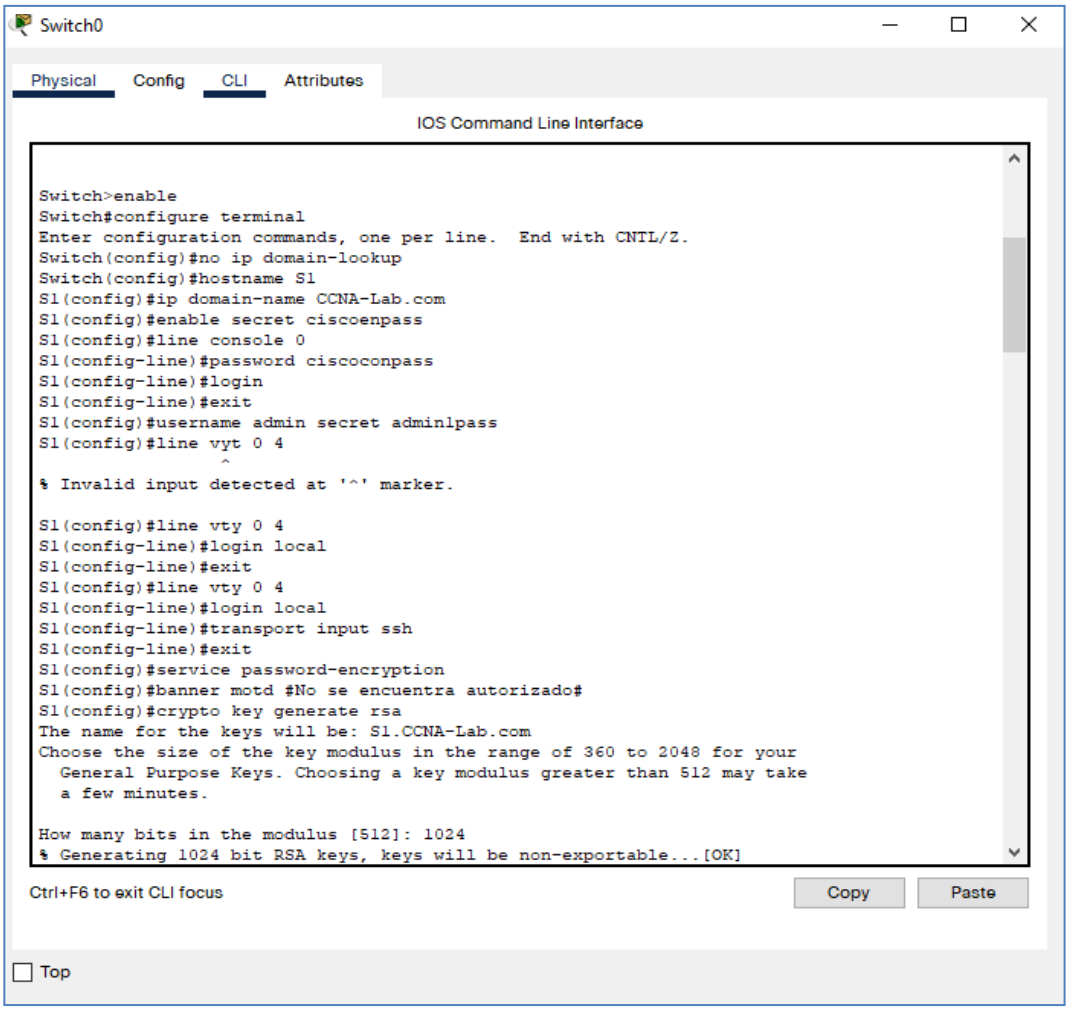
Configuración S1.	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS. Nombre del switch	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	Switch(config)#no ip domain-lookup Switch(config)#hostname S1
Nombre de dominio ccna-lab.com	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 S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 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 4 S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #No se encuentra autorizado#
Generar una clave de cifrado RSA	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]
Configurar la interfaz de administración (SVI)	S1(config)#int vlan 1 *Mar 1 2:24:34.900: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 192.168.49.2 255.255.255.128 S1(config-if)#no shutdown

	S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 192.168.49.1

Ilustraciones de configuración aplicada Switch S1.

Ilustración 5. Configuración S1



Fuente: Elaboración propia.

Paso 2: Configurar los PC

Detalle de direccionamiento IP para los equipos PC A y B

Tabla 5. Configuración PC1

PC-A Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	000D.BD7D.B5CA
Dirección IP	169.254.181.202
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0

Tabla 6. Configuración PC 2

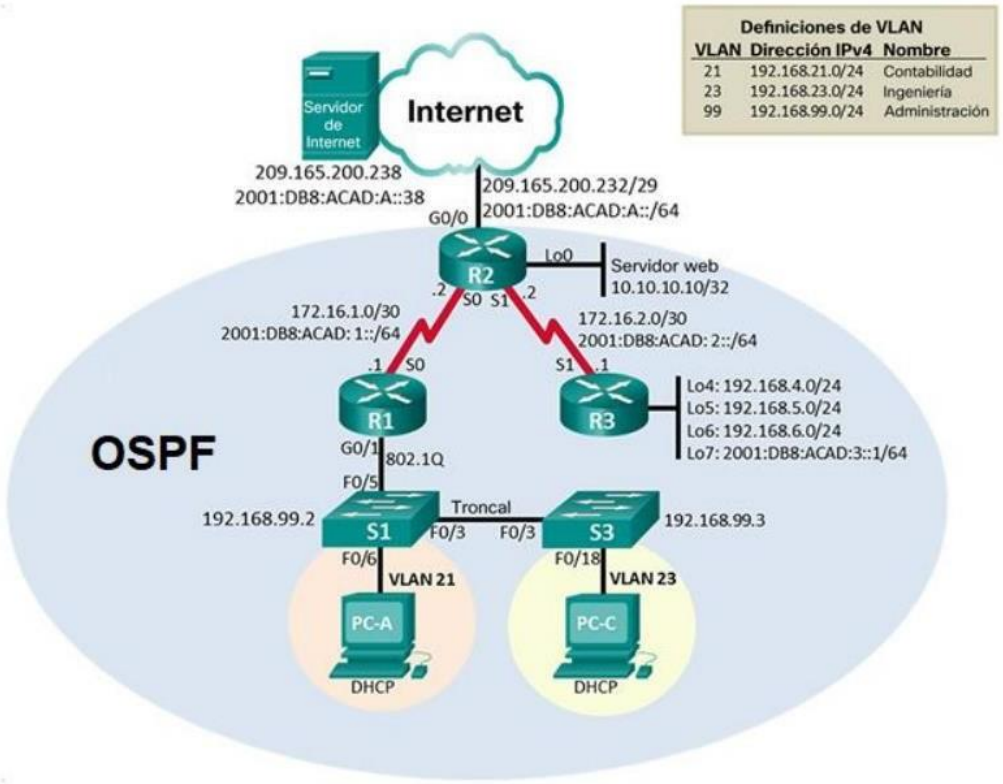
PC-B Network Configuration	
Descripción	FastEthernet0 Connection:(default port)
Dirección física	000C.851A.445B
Dirección IP	169.254.68.91
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0

ESCENARIO 2

Configuración 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.

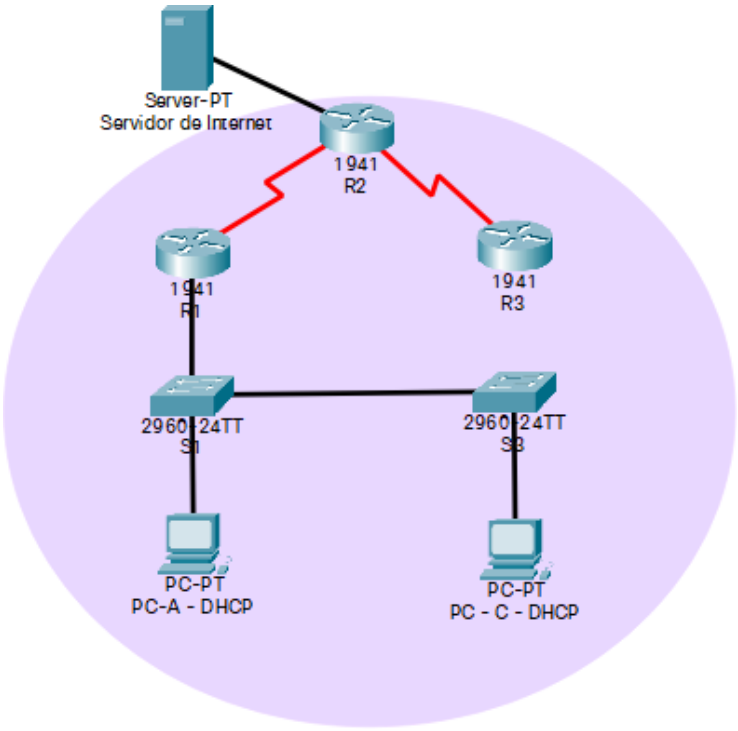
Ilustración 6. Topología propuesta



Fuente: Academia Cisco

Construcción de Red.

Ilustración 7 Construcción de Red Packet Tracer



Fuente: Elaboración propia.

Esquema de direccionamiento

Tabla 7. Esquema de direccionamiento

Dispositivo	Dirección IP
Servidor de Internet	209.165.200.238 2001:DB8:ACAD:A::38
R1	172.16.1.0/30 2001:DB8:ACAD:1::/64
R2	209.165.200.232//29 2001:DB8:ACAD:A::/64
R2- Lo0 (servidor web)	10.10.10.10/30
R3	172.16.2.0/30 2001:DB8:ACAD:2::64
R3- Lo4	192.168.4.0/24
R3- Lo5	192.168.5.0/24

R3- Lo6	192.168.6.0/24
R3- Lo7	192.168.7.0/24
S1	192.168.99.2
S3	192.168.99.3

Inicialización de Dispositivos

A continuación, se inicializan los dispositivos, para ello procedemos a borrar configuración previa y ejecutamos reinicio.

Tabla 8. Inicialización de dispositivos

Configuración **Router/Switchs**	
Requerimiento	Instrucciones (comandos)
Eliminar el archivo startup-config de todos los routers	Router>enable 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>enable Switch #erase startup-config Switch #delete 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>enable Switch#show flash

Ilustraciones de reinicio de dispositivos

Ilustración 8 Inicialización de Routers

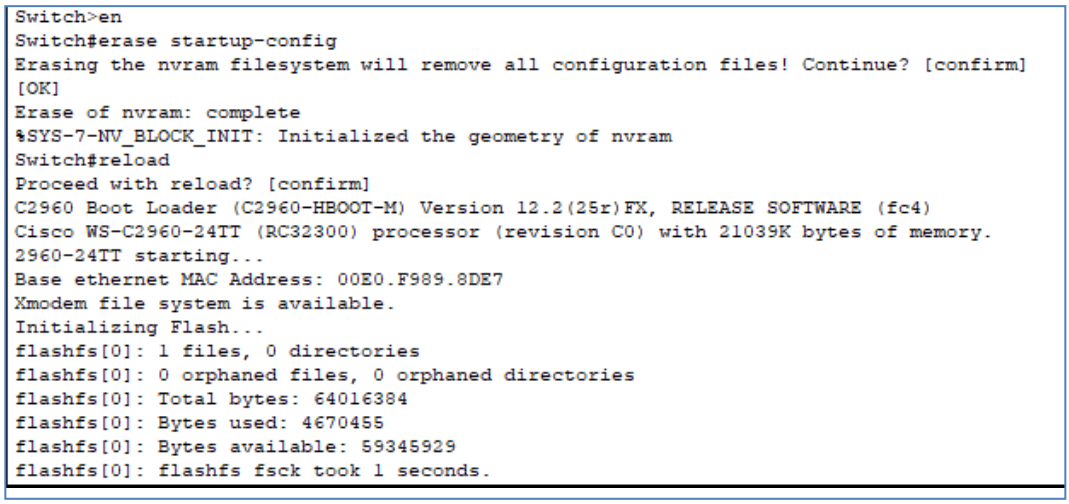
```
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
```

Fuente: Elaboración propia.

Ilustración 9. Inicialización de Switchs



Fuente: Elaboración propia.

Configuración Básica de Dispositivos

Configuración de red en servidor.

Tabla 9. Configuración Servidor

Elemento	Configuración
Dirección IPv4	209.165.200.238
Máscara de subred IPv4	255.255.255.248
Gateway predeterminado IPv4	209.165.200.225
Dirección IPv6	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

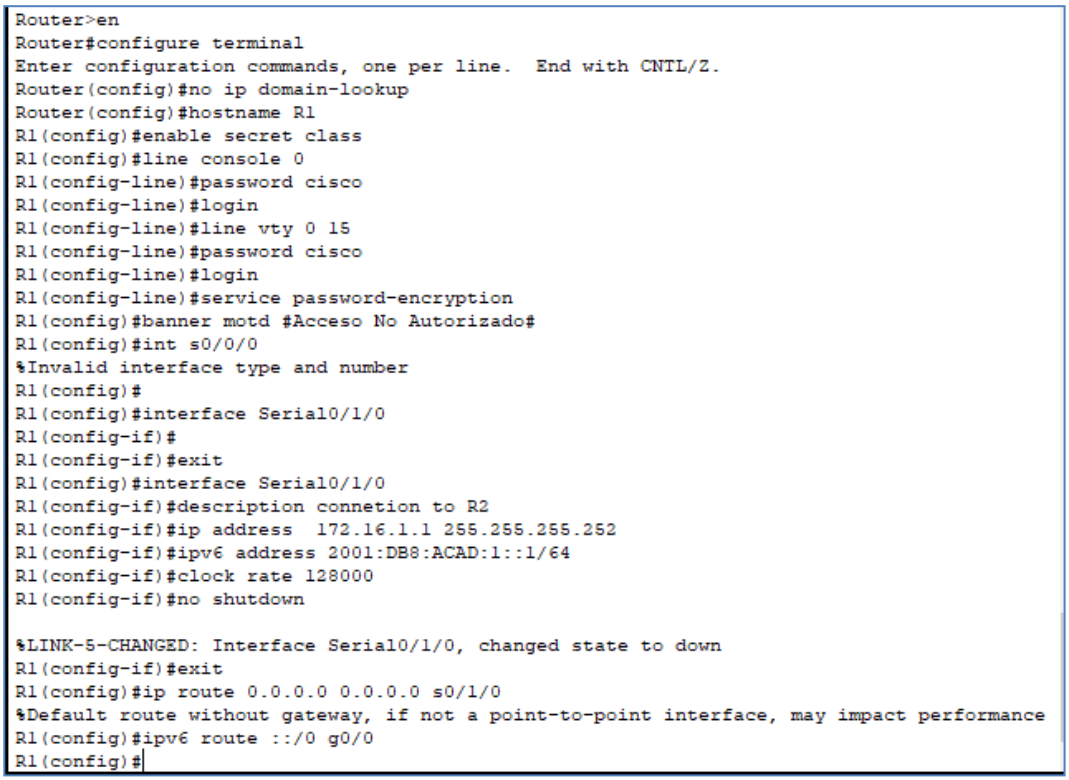
Configuración básica de Router 1 mediante comandos de consola (CLI)

Tabla 10. Configuración R1

Configuración **R1.**	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router R1	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
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #Acceso No Autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description connection to 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
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R2(config-if)#ipv6 route ::/0 g0/0

Ilustraciones de configuración R1.

Ilustración 10. Configuración R1



```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd #Acceso No Autorizado#
R1(config)#int s0/0/0
%Invalid interface type and number
R1(config)#
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#description connetion to 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

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 g0/0
R1(config)#
```

Fuente: Elaboración propia.

Configuración básica de Router 2 mediante comandos de consola (CLI)

Tabla 11. Configuración R2

Configuración **R2.**	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router R2	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
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server (Este commando no funciona en Packet Tracer)
Mensaje MOTD	R2(config)#banner motd #Acceso No Autorizado#
Interfaz S0/1/0	R2(config)#int s0/1/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz S0/1/1	R2(config)#int s0/1/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int l0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated web server R2(config-if)#exit
Rutas predeterminadas	R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config-if)#ipv6 route ::/0 g0/0

Ilustraciones de configuración R2.

Ilustración 11. Configuración R2

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#ip http server
                ^
% Invalid input detected at '^' marker.

R2(config)#banner motd #Acceso No Autorizado#
R2(config)#int s0/1/0
R2(config-if)#description connection to R1
R2(config-if)#ip address 172.16.1.2
% Incomplete command.
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 Serial0/1/0, changed state to up

R2(config-if)#exit
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R2(config)#int s0/1/1
R2(config-if)#description connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
```

Fuente: Elaboración propia.

Configuración básica de Router 3 mediante comandos de consola (CLI)

Tabla 12. Configuración R3

Configuración **R3.**	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router R3	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class

Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Acceso No Autorizado#
Interfaz S0/1/1	R3(config)#int s0/1/1 R3(config-if)#description connection to 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)#clock rate 128000 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int lo 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int lo 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int lo 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int lo 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/1/1 R3(config)#ipv6 route ::/0 s0/1/1

Ilustraciones de configuración R3.

Ilustración 12 Configuración R3

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd #Acceso No Autorizado#
R3(config)#int s0/0/1
%Invalid interface type and number
R3(config)#int s0/1/1
R3(config-if)#description connection to 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)#clock rate 128000
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

R3(config-if)#int lo 4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
```

Fuente: Elaboración propia.

Configuración básica de Switch 1 mediante comandos de consola (CLI)

Tabla 13 Configuración S1

Configuración **S1**	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	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
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line) #service password-encryption
Mensaje MOTD	S1(config)#banner motd #Acceso No Autorizado#

Ilustraciones de configuración S1.

Ilustración 13. Configuración S1

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console
% Incomplete command.
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #Acceso No Autorizado#
S1(config)#
```

Fuente: Elaboración propia.

Configuración básica de Switch 3 mediante comandos de consola (CLI)

Tabla 14 Configuración S3

Configuración **S3**	
Requerimiento	Instrucciones (comandos)
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	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
Contraseña de acceso Telnet	S3(config-line)#line vty 0 15

	S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line) #service password-encryption
Mensaje MOTD	S3(config)#banner motd #Acceso No Autorizado#

Ilustración 14 Configuración S3

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #Acceso No Autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente: Elaboración propia.

Verificar conectividad de la red

Validación de conexión mediante comando ping entre routers y PC de internet

Tabla 15 Validación de conexión mediante ping

Desde	A	Dirección IP	Resultado
R1	R2, S0/1/0	172.16.1.2	R1#ping 172.16.1.2
R2	R3, S0/1/1	172.16.2.1	R2#ping 172.16.2.1
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233

Resultado de ping.

Ilustración 15 Ping R1 a 172.16.1.2

```
R1>en
Password:
R1#ping 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 = 5/6/8 ms

R1#
```

Fuente: Elaboración propia.

Ilustración 16 Ping R2 a 172.16.2.1

```
R2>en
Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
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 = 4/5/7 ms

R2#
```

Fuente: Elaboración propia.

Ilustración 17 Ping desde servidor a 209.165.200.233

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 209.165.200.233

Pinging 209.165.200.233 with 32 bytes of data:

Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time=6ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Fuente: Elaboración propia.

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

Creación de VLANs y asignación de direcciones IP en Switch 1 mediante comandos de consola (CLI)

Tabla 16 Configuración seguridad y VLAN S1

Configuración **S1**	
Requerimiento	Instrucciones (comandos)
Crear la base de datos de VLAN	S1#configure terminal 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)#int vlan 99 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)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Ilustración 18. Configuración seguridad y vlan S1

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#int 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)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
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)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
```

Fuente: Elaboración propia.

Creación de VLANs y asignación de direcciones IP en Switch 3 mediante comandos de consola (CLI)

Tabla 17 Configuración Seguridad Vlan S3

Configuración **S3**	
Requerimiento	Instrucciones (comandos)
Crear la base de datos de VLAN	S3#configure terminal 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

Asignar la dirección IP de administración.	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Ilustración 19 Configuración Seguridad y VLAN S3

```
S3>en
Password:
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#int 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)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

Fuente: Elaboración propia.

Configuración de subinterfaces en Router 1 mediante comandos de consola (CLI)

Tabla 18 Configuración seguridad y subinerfaces R1

Configuración R1	
Requerimiento	Instrucciones (comandos)
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

Ilustración 20 Configuración seguridad y VLAN R1

```
R1>en
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown
```

Fuente: Elaboración propia.

Verificar conectividad de la red

Validación de conexión mediante comando ping entre switch y routers.

Tabla 19. Verificación de conectividad

Desde	A	Dirección IP	Resultado
S1	R1, dirección VLAN 99	192.168.99.1	S1#Ping 192.168.99.1
S3	R1, dirección VLAN 99	192.168.99.1	S3#Ping 192.168.99.1
S1	R1, dirección VLAN 21	192.168.21.1	S1#Ping 192.168.21.1
S3	R1, dirección VLAN 23	192.168.23.1	S3#Ping 192.168.23.1

Resultado de ping.

Ilustración 21. Ping 192.168.99.1 desde S1

```
S1>en
Password:
Password:
S1#ping 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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: Elaboración propia.

Ilustración 22 Ping 192.168.99.1 desde S3

```
S3#ping 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 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms
```

Fuente: Elaboración propia.

Ilustración 23 Ping 192.168.21.1 desde S1

```
S1#ping 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 = 0/0/4 ms
```

Fuente: Elaboración propia.

Ilustración 24. Ping 192.168.23.1 desde S3

```
S3#ping 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
```

Fuente: Elaboración propia.

Configurar el protocolo de routing dinámico OSPF

Configuración de protocolo OSPF para Router 1.

Tabla 20 Configuraciòn OSPF R1

Configuración **R1**	
Elemento	**Instrucciones (comandos)**
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.255 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
Anunciar las redes conectadas directamente	R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 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

Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Ilustración 25. Configuraciòn OSPF R1

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.0 0.0.0.255 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
R1(config-router)#do show ip route connected
 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)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
```

Fuente: Elaboración propia.

Configuración de protocolo OSPF para Router 2.

Tabla 21 Configuración OSPF R2

Configuración **R2**	
Elemento	**Instrucciones (comandos)**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 17:47:56: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/0/0router ospf 1 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
Anunciar las redes conectadas directamente	R2(config-router)#do show ip route connected C 10.10.10.10/32 is directly connected, Loopback0 C 172.16.1.0/30 is directly connected, Serial0/0/0

	C 172.16.2.0/30 is directly connected, Serial0/0/1
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática	R2(config-router)#no auto-summary

Ilustración 26 Configuración OSPF R2

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.10 0.0.0.255 area 0
R2(config-router)#network 172.16.1.0 0.0.0.255 area 0
R2(config-router)#
20:47:54: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on Serial0/1/0 from LOADING to
FULL, Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.255 area 0
R2(config-router)#do show ip route connected
 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)#router ospf 1
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
```

Fuente: Elaboración propia.

Configuración de protocolo OSPF para Router 3.

Tabla 22 Configuración OSPF R3

Configuración **R3**	
Elemento	**Instrucciones (comandos)**
Configurar OSPF área 0	R3(config)#router ospf 1 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
Anunciar las redes conectadas directamente	R3(config-router)#do show ip route connected C 172.16.2.0/30 is directly connected, Serial0/0/1 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
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6

Desactive la sumarización automática	R3(config-router)#no auto-summary

Ilustración 27 Configuración OSPF R3

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
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
R3(config-router)#do show ip route connected
 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)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
```

Fuente: Elaboración propia.

Verificar información de OSPF

Tabla 23 Verificación información de 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 1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#Show run | section router ospf 1

Ilustración 28. Verificar protocolo OSPF

```
R3#Show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.6.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.6.1           110      00:29:19
  Distance: (default is 110)

R3#Show ip route ospf 1
R3#Show run | section router ospf 1
router ospf 1
 log-adjacency-changes
 passive-interface Loopback4
 passive-interface Loopback5
 passive-interface Loopback6
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
R3#
```

Fuente: Elaboración propia.

Implementar DHCP y NAT para IPv4

Configurar el router R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 24 Configurar el R1 como servidor de DHCP

Elemento	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)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1

	R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccnasa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10

Ilustración 29 Configurar el R1 como servidor de DHCP

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccnasa.com
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#exit
R1(config)#
```

Fuente: Elaboración propia.

Configurar la NAT estática y dinámica en el R2

Tabla 25 Configurar la NAT estática y dinámica en el R2

Elemento	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (no soportado)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
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 s0/1/0 R2(config-if)#ip nat inside R2(config-if)#int s0/1/1 R2(config-if)#ip nat inside
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 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Ilustración 30 Configurar la NAT estática y dinámica en el R2

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip http server
                ^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
                ^
% Invalid input detected at '^' marker.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/1/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/1/1
R2(config-if)#ip nat inside
R2(config-if)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
```

Fuente: Elaboración propia.

Verificar el protocolo DHCP y la NAT estática

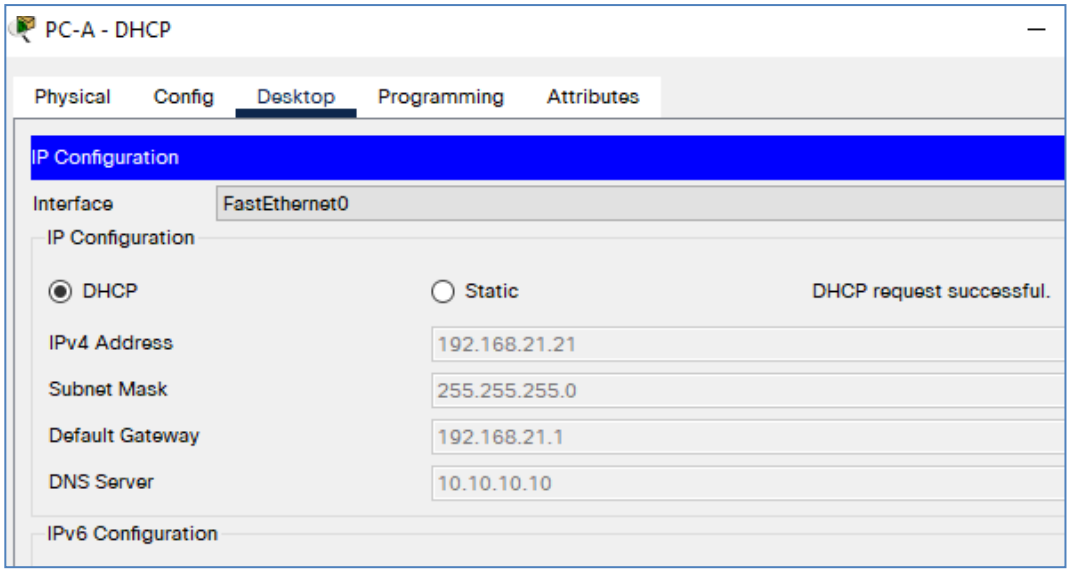
Proceso para validar la conectividad una vez se ha establecido el protocolo DHCP y se ha designado la configuración NAT.

Tabla 26. Verificación protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso, fue asignada la dirección 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso, fue asignada la dirección 192.168.23.21
Verificar que la PC-A pueda hacer ping a la PC-C	Ping Exitoso

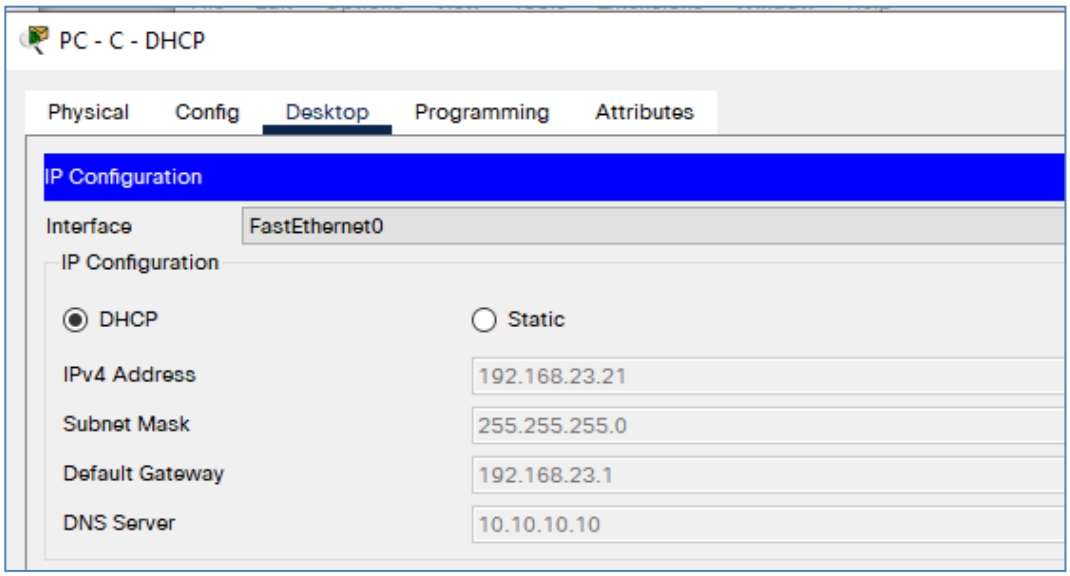
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	Server Reset Connection

Ilustración 31 Asignación dinámica PC-A



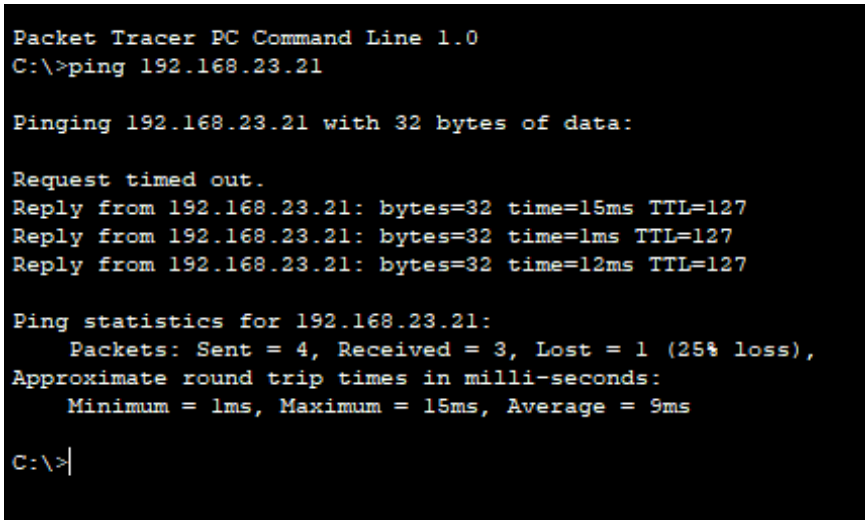
Fuente: Elaboración propia

Ilustración 32 Asignación dinámica PC-C



Fuente: Elaboración propia

Ilustración 33 Ping entre PC-A y PC-C



Fuente: Elaboración propia.

Configurar NTP

Configuración en routers R1 y R2 para sincronización de fecha y hora mediante el protocolo NTP, en este caso definimos a R2 como servidor.

Tabla 27 Configuración NTP

Elemento	Especificación
Ajuste la fecha y hora en R2	R2#clock set 09:00:00 05 mar 2016
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 updatecalendar
Verifique la configuración de NTP en R1	R1#show ntp associations

Ilustración 34 Configuración NTP

```
R2>en
Password:
R2#clock set 09:00:00 05 mar 2016
R2#ntp master 5
       ^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp master 5
```

Fuente: Elaboración propia.

Ilustración 35 Show NTP Associations

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay          offset
disp
*~172.16.1.2    127.127.1.1     5    14       16      1      4.00           0.00
0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1#
```

Fuente: Elaboración propia.

Configurar y verificar las listas de control de acceso (ACL)

Configuración de listas de acceso y restricción a las líneas VTY

Tabla 28 Restringir acceso a lineas VTY en R2

Elemento	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
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado User Access Verification Password: R2>

Ilustración 36 Restringir acceso a lineas VTY en R2

```
R2#en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
```

Fuente: Elaboración propia.

Ilustración 37 Verificación ACL

```
R1>en
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenAcceso No Autorizado


User Access Verification

Password:
```

Fuente: Elaboración propia.

Verificación de las ACL

Tabla 29 verificación de las ACL

Elemento	Entrada
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list 1 Standard IP access list 1 permit 0.0.0.7 255.255.255.248 permit 192.168.21.0 0.0.0.255 permit 192.168.23.0 0.0.0.255 permit 192.168.4.0 0.0.0.255 permit 192.168.4.0 0.0.3.255
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Ilustración 38 show access-list 1

```
R2#show access-list 1
Standard IP access list 1
    permit 192.168.21.0 0.0.0.255
    permit 192.168.23.0 0.0.0.255
    permit 192.168.4.0 0.0.3.255

R2#clear access-list counters
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
```

Fuente: Elaboración propia.

Ilustración 39 show ip nat translations

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.229   10.10.10.10        ---                ---
tcp 209.165.200.229:80 10.10.10.10:80     209.165.200.238:1025209.165.200.238:1025
```

Fuente: Elaboración propia.

CONCLUSIONES

Como resultado del ejercicio realizado se tiene la consolidación de conceptos de administración de dispositivos principales para la instalación de redes, aplicación de patrones de seguridad como exigencia de claves y encriptación de estas, con el apoyo de la herramienta packet tracer se logra simular de manera exitosa la manipulación de dispositivos y la asignación de segmentos de red para cada vlan o subred implementada.

A nivel de conocimiento se logra profundizar la temática de cálculo de direccionamiento IP de acuerdo con un segmento propuesto, para el caso de estudio los últimos números del documento del estudiante.

Dentro del desarrollo de la práctica de escenario dos se profundiza el conocimiento adquirido con la aplicación de protocolo de routing dinámico OSPF y en gran parte muestra el apoyo que esto podría dar en la configuración de redes ya que se evita la administración manual de direcciones IP para cada dispositivo, como el enrutamiento de redes externas a internas con protocolo NAT.

BIBLIOGRÁFIA

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: 56g CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

Ejemplo de configuración de OSPF con adyacencia multiárea. (2019, 23 diciembre). Cisco. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html