SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE LA TECNOLOGIA CISCO

CRISTHIAN MAURICIO RAMIREZ MESA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI

INGENIERIA DE SISTEMAS

GIRARDOT – CUNDINAMARCA

2022

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE LA TECNOLOGIA CISCO

CRISTHIAN MAURICIO RAMIREZ MESA

Diplomado de opción de grado presentado para optar por el título de ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE SISTEMAS
GIRARDOT – CUNDINAMARCA
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Girardot, 26 de junio de 2022

AGRADECIMIENTOS

Quiero agradecer a toda mi familia, a mis padres y a mi esposa por el apoyo incondicional que siempre me han brindado en todos los proyectos y demás metas que me he trazado en la vida, a pesar de la distancia, siempre sentí su mano protectora y su voz de aliento y respaldo, siempre los he sentido aquí a mi lado.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP (Dynamic Host Configuration Protocol). DHCP es un protocolo de configuración que asigna de forma dinámica direcciones IP para clientes. Funciona en versión DHCPv4 y DHCPv6.

INTERFAZ. “Puertos especializados en un dispositivo de red que se conecta a redes individuales.

LAN. Una LAN (Local Area Network) es una infraestructura de la red cuyo alcance se restringe a un área geográfica pequeña, como una oficina, un edificio, un hotel o un campus universitario.

MÁSCARA DE SUBRED IPv4. “Una máscara de subred IPv4 es un valor de 32 bits que separa la porción de red de la dirección de la porción de host. Junto con la dirección IPv4, la máscara de subred determina a qué subred pertenece el dispositivo.

NAT (Network Address Translation) La Traducción de Direcciones de Red se utiliza para “Traducir las direcciones IPv4 de una red privada en direcciones IPv4 públicas globalmente únicas

NTP (Network Time Protocol). Protocolo que se utiliza para sincronizar los relojes de los sistemas informáticos a través de redes de datos de latencia variable conmutadas por paquetes

OSPF (Open Shortest Path First). Es un protocolo de enrutamiento de estándar abierto, de tipo pasarela interior (IGP), que permite encontrar el camino más corto entre dos hosts

TOPOLOGÍA FÍSICA. “Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación del cable

RESUMEN

En este documento se ponen a prueba las habilidades prácticas obtenidas por el estudiante en el Diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN)

El protocolo de enrutamiento a utilizar en este escenario será el OSPF, teniendo en cuenta que posee rutas distribuidas por defecto, asimismo se realiza la configuración del encapsulamiento PPP y su respectiva autenticación, también se muestra el proceso de configuración para proporcionar el servicio DHCP a la propia red LAN y los routers de cada ciudad, para terminar se realiza la configuración de de PPP en los enlaces hacia el ISP con su respectiva autenticación y la traducción de direcciones de red dinámicas y estáticas NAT de sobrecarga en dos de los routers

PALABRAS CLAVE: CONFIGURACIÓN, DHCP, ROUTER, RUTAS, SIMULADOR.

ABSTRACT

In this document, the practical skills obtained by the student in the Cisco Deepening Diploma (Design and implementation of integrated LAN / WAN solutions)

The routing protocol to be used in this scenario will be the OSPF, taking into account that it has distributed routes by default, the PPP encapsulation configuration and its respective authentication are also performed, the configuration process is also shown to provide the DHCP service to the LAN network and the routers of each city, to finish, the PPP configuration is made in the links to the ISP with their respective authentication and the translation of dynamic and static network addresses overload NAT in two of the routers

KEY WORDS: CONFIGURATION, DHCP, ROUTER, ROUTES, SIMULATOR.

INTRODUCCION

La innovación tecnológica en todos los campos especialmente en las telecomunicaciones y la informática han transformado nuestro entorno y generado una revolución en todos los campos de nuestra vida cotidiana y laboral. Esta transformación abarca las organizaciones donde nos desenvolvemos implicando cambios en las relaciones entre estas y su entorno, generando un rediseño de las estructuras de dichas organizaciones y redefiniendo las relaciones tanto laborales como industriales.

En este sentido es importante por medio de la profundización en CCNA desarrollar las competencias y poner en práctica las habilidades aprendidas aplicándolas en la resolución de problemas derivados del uso de las Networking, que como se mencionó anteriormente tienen una aplicación y transformación directa del entorno organizacional donde nos desenvolvemos.
Así mismo la aplicación de escenarios LAN Y WAN permitirán analizar y entender que tan efectivos son los protocolos que por medio de comandos específicos evalúan el desempeño de routers y switches.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Desarrollar los ejercicios prácticos propuestos en la Guía de Trabajo denominada “Prueba de habilidades CCNA 2022”, según los requerimientos de la “Guía de actividades - Unidad 5 - Paso 6 - Entrega Avance Documento Final”.

2.2. OBJETIVOS ESPECÍFICOS

Desarrollar el Escenario 1 propuesto de forma tal que la red sea completamente operativa en el simulador de Cisco Packet Tracer.

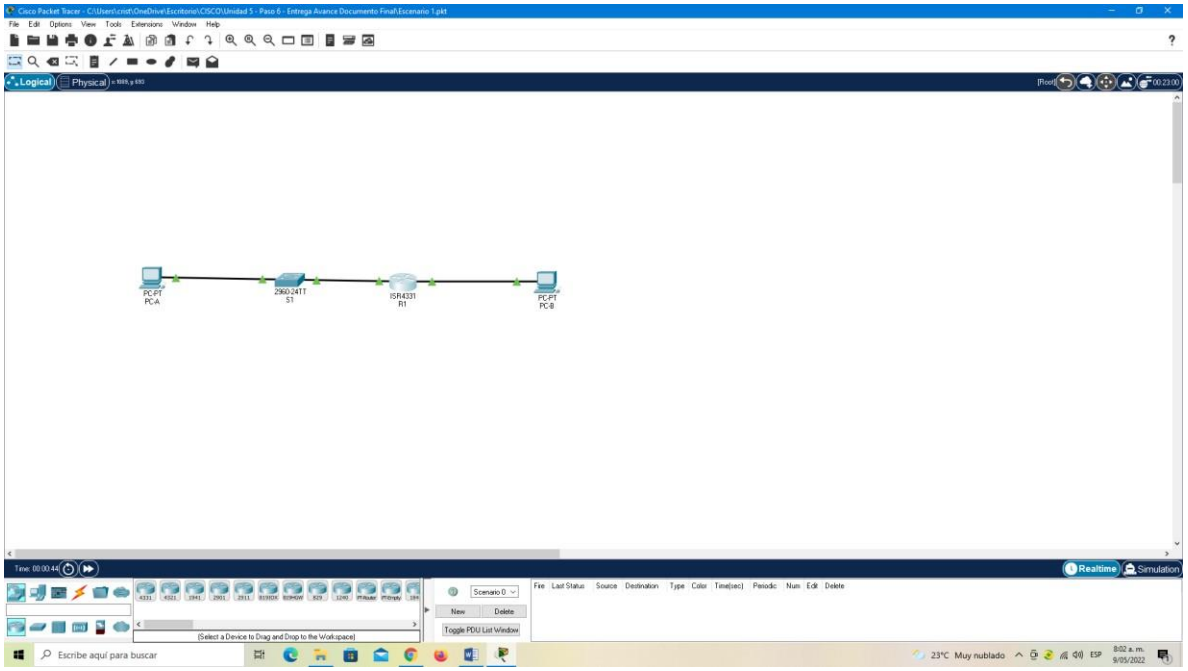
Desarrollar, usando el simulador de Cisco Packet Tracer, el Escenario 2 propuesto de forma tal que se cumplan con todos los requerimientos de configuración solicitados.

Presentar evidencia del correcto funcionamiento de los equipos, según las configuraciones realizadas.

ESCENARIO 1

Figura 1: Topología scenario 1

Figura 1 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.

Objetivos

Parte 1: Construir en el simulador la Red

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

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

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

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

Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el 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.

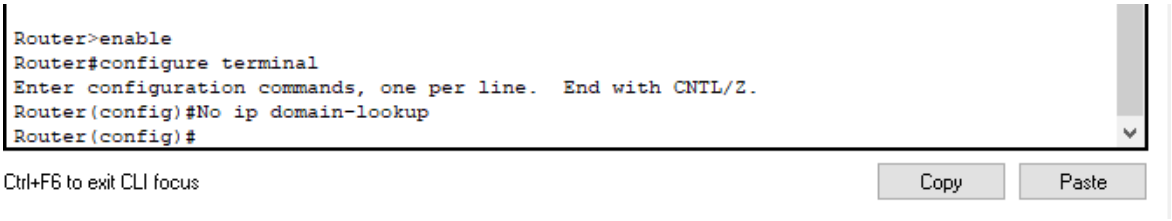
Tabla 1. Tareas de configuración para R1

TAREA	DESCRIPCION
Deshabilitar de las búsqueda DNS en R1	➢ Router> ➢ Router>enable **Ingreso al modo privilegiado** ➢ Router#configure terminal **Ingreso al modo de configuración** ➢ Router(config)# No ip domain-lookup **Desactivamos las búsquedas DNS**
Nombre del Router	En modo de configuración se coloca el comando para asignarle el nombre al Router • Router(config)#hostname R1
Nombre de dominio	Se configura se coloca el comando para asignarle el nombre de dominio • Router(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado • R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola asi: R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer las contraseñas	Se configura el comando para que se establezca la longitud mínima para las contraseñas de 10 caracteres R1(config)# security passwords min-length
Crear un usuario administrativo en la base de datos local	Se configura el comando para crear un usuario administrativo en el BD local con el Nombre: admin y la contraseña: admin1pass asi: R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las	Se configura inicio de la sesión en las líneas VTY admin y la contraseña:

líneas VTY para que use la base de datos local	• R1(config)#line vty 0 4 • R1(config-line)#login local
Configurar VTY solo aceptando SSH	Se configura el comandoVTY solo aceptando SSH • R1(config-line)#transport input ssh • R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Se configura el comando para poder cifrar las contraseñas de texto no cifrado • R1(config)#service password-encryption
Configuración del mensaje (MOTD)	Se configura se coloca el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado • R1(config)#banner motd**"El Acceso al router es restringido. Únicamente personal autorizado"**
Habilitar el routing IPv6	Se configura el comando para Habilitar el routing IPv6 • R1(config)#ipv6 unicast-routing
Configuración interface gigabitethernet 0/0/0	Se configura el comando para la interface gigabitethernet 0/0/0: • R1(config)# interfaz g0/0/0 Se configura la interface G 0/0 • R1(config-if)# ip address 192.168.80.129 255.255.255.192 • R1(config-if)# no shutdown
Configuración interface gigabitethernet 0/0/1	Se configura el comando para la interface gigabitethernet 0/0/0 • R1(config)# interfaz g0/0/1 Se configura la interfaz G 0/0/1 • R1(config-if)# ip address 192.168.80.1 255.255.255.128 • R1(config-if)# no shutdown
Generamos una clave de cifrado RSA	Se configura el comando para la generación una clave de cifrado RSA: • R1(config)#crypto key generate rsa • How many bits in the modulus [512]: 1024 • R1(config)#exit

- Router>
- Router>enable **Ingreso al modo privilegiado**
- Router#configure terminal **Ingreso al modo de configuración**
- Router(config)# No ip domain-lookup **Desactivamos las búsquedas DNS**

Figura 4 DESHABILITAR DE LAS BÚSQUEDA DNS EN R1



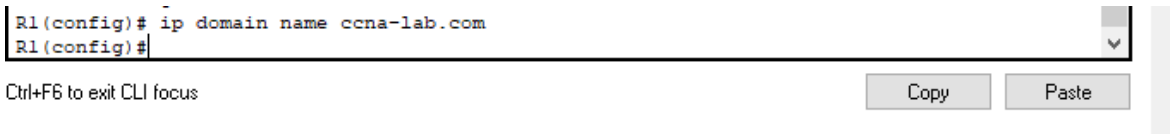
- Se asigna nombre al router **Router(config)#hostname R1**

Figura 5. NOMBRE DEL ROUTER

```
Router>
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
```

- Se asigna nombre de dominio con el comando R1(config)# ip domain name ccna-lab.com

Figura 6 DOMINIO DE ROUTER



- Se asigna contraseña EXEC en modo privilegiado

R1(config)# enable password ciscoconpass

- Se crea contraseña de acceso a la consola

R1(config)# line console 0
R1(config)# password ciscoenpass

R1(config)# login

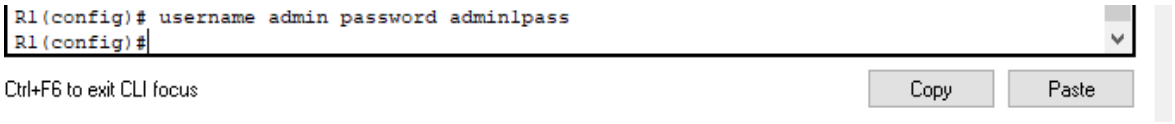
- Se establece longitud mínima para las contraseñas

R1(config)# security password min-length 10

- Se crea un usuario administrativo en la BD local

R1(config)# username admin password admin1pass

Figura 7 ASIGNACIÓN CLAVES DE ACCESO



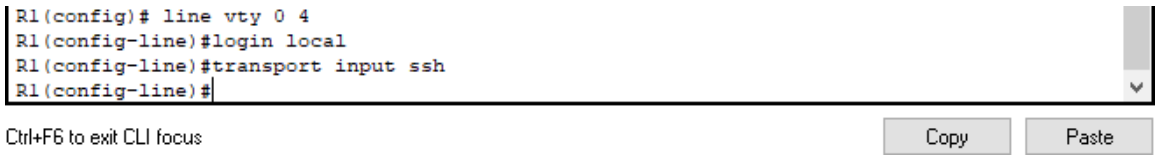
- Se configuro inicio de sesión de las líneas VTY para el uso de bases de datos local

R1(config)# line vty 0 4
R1(config)# login local

- Se configuro vty solo acepta SSH

R1(config)# transport input ssh

Figura 8 CONFIGURACIÓN DE LOS PUERTOS SERIALES DE R1



- Se cifra las contraseñas de texto

R1(config)# service password-encryption

- Configurar el motd banner

R1(config)# banner motd "El Acceso al router es restringido.
Únicamente personal autorizado"

Figura 9. SOLICITUD DE CREDENCIALES DE ACCESO

```
R1(config-line)#service password-encryption
R1(config)# banner motd ''el acceso al router es restringuido. Unicamente personal
autorizado''
R1(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

- Se configura la interface gigabitethernet 0/0/0

R1(config)# interfaz gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.80.129 255.255.255.192
R1(config-if)# no shutdown

- Se configura la interface gigabitethernet 0/0/1

R1(config)# interfaz gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.80.1 255.255.255.128
R1(config-if)# no shutdown

Figura 10. CONFIGURACIÓN DE LOS PUERTOS GIGABITETHERNET DE R1

```
R1(config)#interface gigabitethernet 0/0/0
R1(config-if)#ip address 192.168.80.129 255.255.255.192
R1(config-if)#no shut
R1(config-if)#interface gigabitethernet 0/0/1
R1(config-if)#ip addres 192.168.80.1 255.255.255.128
R1(config-if)#no shut
R1(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

- Generamos una clave cifrado RSA

R1(config)# ip domain-name ccna-lab.com
R1(config)# crypto key generate rsa
How many bits in the modulus [512]:

Figura 11. GENERA CLAVE CIFRADO

```
R1(config-if)#ip domain-name ccna-lab.com
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]:
```

Ctrl+F6 to exit CLI focus Copy Paste

Tabla 2 LAS TAREAS DE CONFIGURACIÓN DEL S1 INCLUYEN:

TAREA	DESCRIPCION
Deshabilitar de las búsqueda DNS en R1	Swicht S1 Swicht>enable **Se ingresa al modo privilegiado** Swicht#configure terminal **Se ingresa al modo privilegiado** Swicht(config)# N ip domain-lookup **Se Desactivan las búsquedas DNS**
Nombre del Swicth	Se configura el comando para asignarle el nombre al Switch Swicht(config)#hostname S1
Nombre de dominio	Se configura el comando para asignarle el nombre de dominio S1(config)# ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado • S1(config)# line console 0 • S1(config)# password ciscoenpass • S1(config)# login • S1(config-line)#exit
Contraseña de acceso a la consola	Se crea un usuario administrativo en la BD local • S1(config)#enable secret ciscoenpass
Crear un usuario administrativo en la base de datos local	Configuracion de comando para crear un usuario administrativo en la BD local. • S1(config)# username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura el comando el inicio en las líneas VTY • S1(config)# line vty 0 4 • S1(config)# login local
Configurar VTY solo aceptando SSH	Se configura VTY solo aceptado SSH • S1(config)# transport input ssh
Cifrar las contraseñas de texto no cifrado	Se cifra las contraseñas de textos S1(config)# service password-encryption
Configuración del mensaje (MOTD)	Se configura el comando para configurar un MOTD Banner con el fin de prohibir el acceso no autorizado

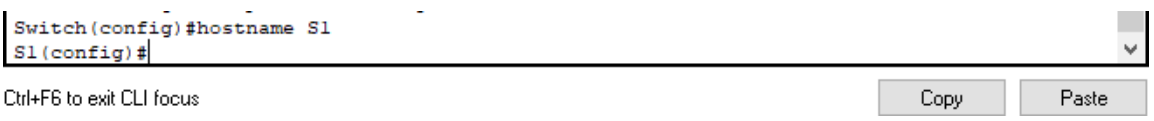
	• S1(config)# banner motd “El Acceso al Router es restringido. Únicamente personal autorizado”
Generamos una clave de cifrado RSA	Se genera una clave de cifrado • S1(config)# crypto key generate rsa • How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	Se configura la interface SVI • S1(config)# interface S1 SVI **utiliza para ingresar ala interfaz** • S1(config-if)# ip address 192.168.80.2 255.255.255.192 **dirección IPv4 de capa 3**
Configurar del Gateway predeterminado	Se configura el Gateway • S1(config-if)# ip address 192.168.80.129 255.255.255.192 • S1(config-if)# no shutdown

Figura 12. DES HABILITACIÓN DE LAS BÚSQUEDAS DNS EN S1

```
Switch#
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#No ip domain-lookup
```

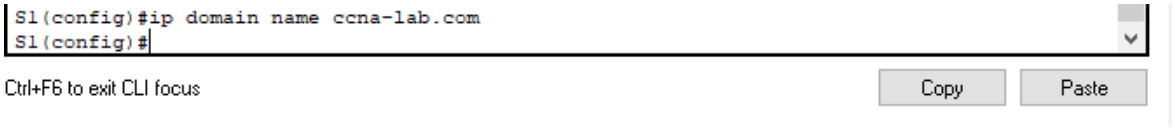
- Se ingresa al modo privilegiado
  Swicht>enable
- Se ingresa al modo de configuración
  Swicht#configure terminal
- Se Desactivan las búsquedas DNS
  Swicht(config)# No ip domain-lookup

Figura 13 NOMBRE DE SWICHT A S1



- Se asigna nombre de dominio
  S1(config)# ip domain name ccna-lab.com

Figura 14. NOMBRE DE DOMINIO DE S1



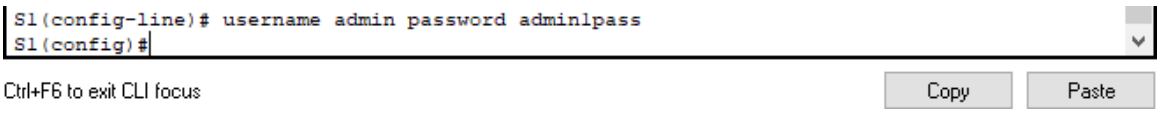
- Se asigno contraseña EXEC en modo privilegiado
  S1(config)# enable password ciscoconpass
- Se crea contraseña de acceso a la consola
  S1(config)# line console 0
  S1(config)# password ciscoenpass
  S1(config)# login

Figura 15. ASIGNACIÓN DE CLAVES DE ACCESO A S1

```
S1(config)#enable password ciscoconpass
S1(config)#line console 0
S1(config-line)# password ciscoenpass
S1(config-line)# login
S1(config-line)#
```

- Se crea un usuario administrativo en la BD local
  S1(config)# username admin password admin1pass

Figura 16 CREAR DE BD LOCAL



- Se configuro inicio de sesión en las líneas VTY para el uso de Bases de Datos LocaL
  S1(config)# line vty 0 4
  S1(config)# login local

- Se Configuro VTY solo aceptando SSH
  S1(config)# transport input ssh

- Se cifra las contraseñas de texto
  S1(config)# service password-encryption

Figura 17. VERIFICACIÓN DE LAS LÍNEAS VTY ACEPTANDO SSH

```
S1(config)# line vty 0 4
S1(config-line)# login local
S1(config-line)#transport input ssh
S1(config-line)#service password-encryption
S1(config)#
```

- Se configuro un motd banner

S1(config)# banner motd “El Acceso al Router es restringido.
Únicamente personal autorizado”

Figura 18. VERIFICACIÓN DEL BANNER MOTD

```
S1(config)#banner motd ''EL ACCESO AL ROUTER ES RESTRINGUIDO. UNICAMENTE PERSONAL
AUTORIZADO''
S1(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

- Se genera una clave de cifrado

S1(config)# ip domain-name ccna-lab.com
S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

Figura 19. VERIFICACIÓN DE CLAVE RSA

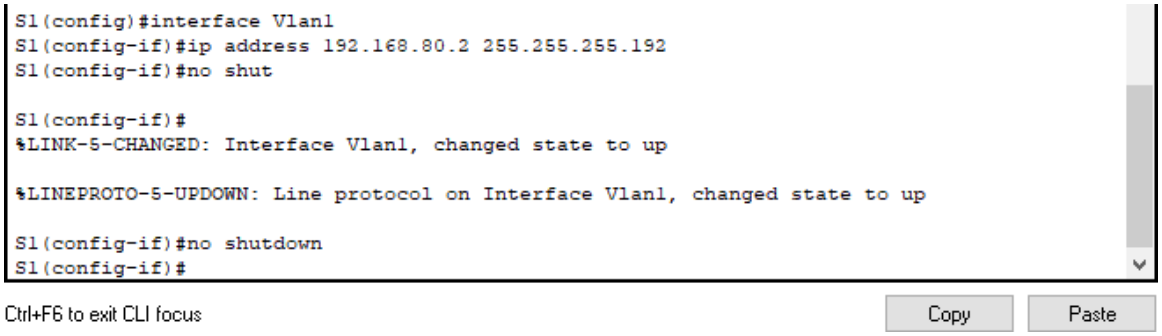
```
S1(config)#ip domain-name ccna-lab.com
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
```

Ctrl+F6 to exit CLI focus Copy Paste

- Se configuro la interface SVI

S1(config)# interface S1 SVI
S1(config-if)# ip address 192.168.80.2 255.255.255.192
S1(config-if)# no shutdown

Figura 20. INTERFACE VLAN 1



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.**80**.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 2. Escenario 1. Requerimientos del modelo.

Item	Requerimiento
Dirección de Red	192.168.**80**.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Item	Requerimiento	Item
Dirección de Red	192.168.**80**.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.**80**.0 donde 80 corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100	192.168.80.0
Requerimiento de host Subred LAN2	50	192.168.80.128

R1 G0/0/1	Primera dirección de host de la subred LAN1	192.168.80.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2	192.168.80.129/26
S1 SVI	Segunda dirección de host de la subred LAN1	192.168.80.2/25
PC-A	Última dirección de host de la subred LAN1	192.168.80.126/25
PC-B	Última dirección de host de la subred LAN2	192.168.80.190/26

PARTE 3: CONFIGURE ASPECTOS BÁSICOS

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

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	**Nombre de usuario: admin Password: admin1pass**
Configurar VTY solo aceptando SSH	**Línea vty 0 4**
Cifrar las contraseñas de texto no cifrado	**Line vty aceptando SSH**
Configure un MOTD Banner	**Ocultar contraseña**
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Las tareas de configuración de S1 incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Linea vty 0 4
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Line vty aceptado SSH
Cifrar las contraseñas de texto no cifrado	Ocultar contraseña
Configurar un MOTD Banner	Mensaje de ingreso
Generar una clave de cifrado RSA	Módulo de 1024 bits
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

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.

PC-A Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	FE80::230:F2FF:FE46:3223
Dirección IP	92.168.80.126
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.80.126

Figura 22. CONFIGURACIÓN DE PC_0

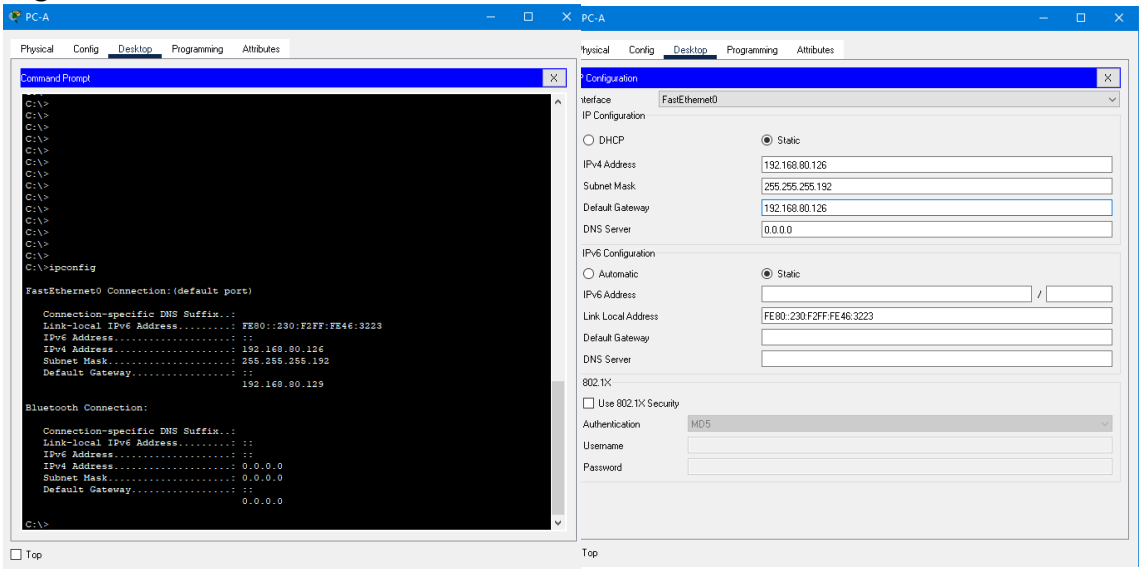
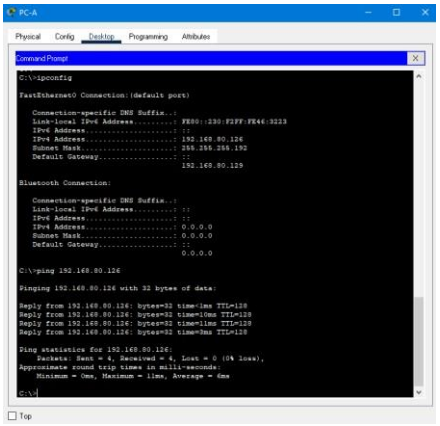
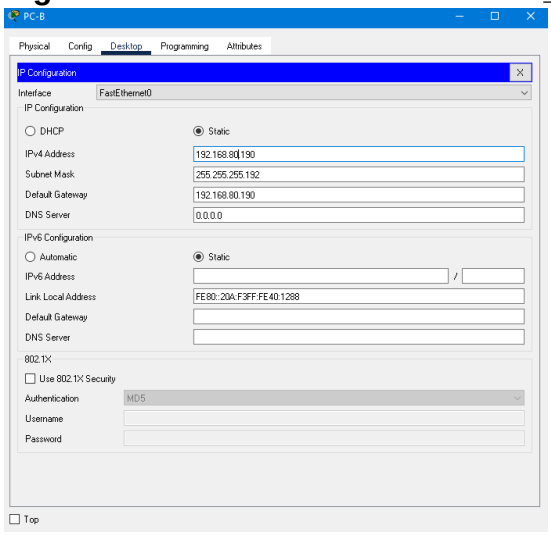


Figura 23. PRUEBA DE CONECTIVIDAD



PC-B Network Configuration	
Descripción	FastEthernet0 connection: (default port)
Dirección física	FE80::20A:F3FF:FE40:1288
Dirección IP	192.168.80.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.80.190

Figura 24. CONFIGURACIÓN DE PC_1



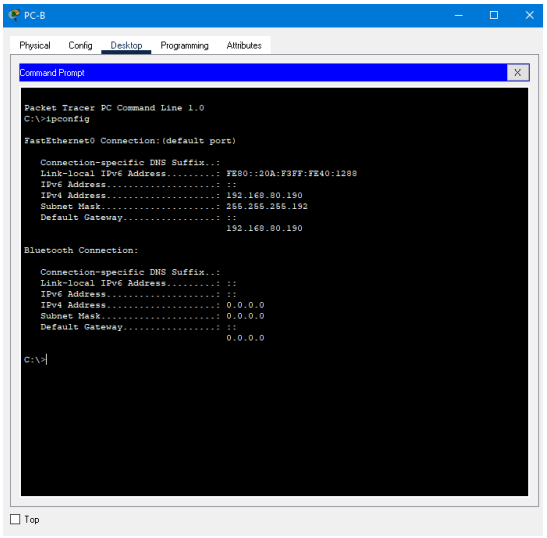
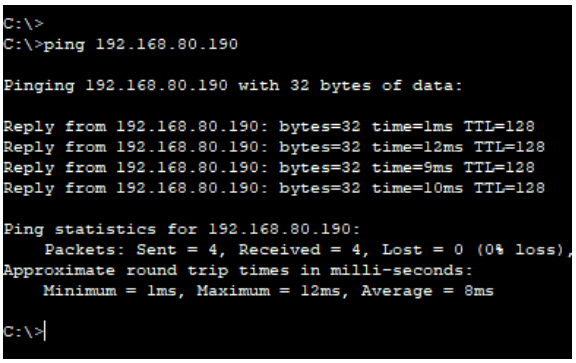


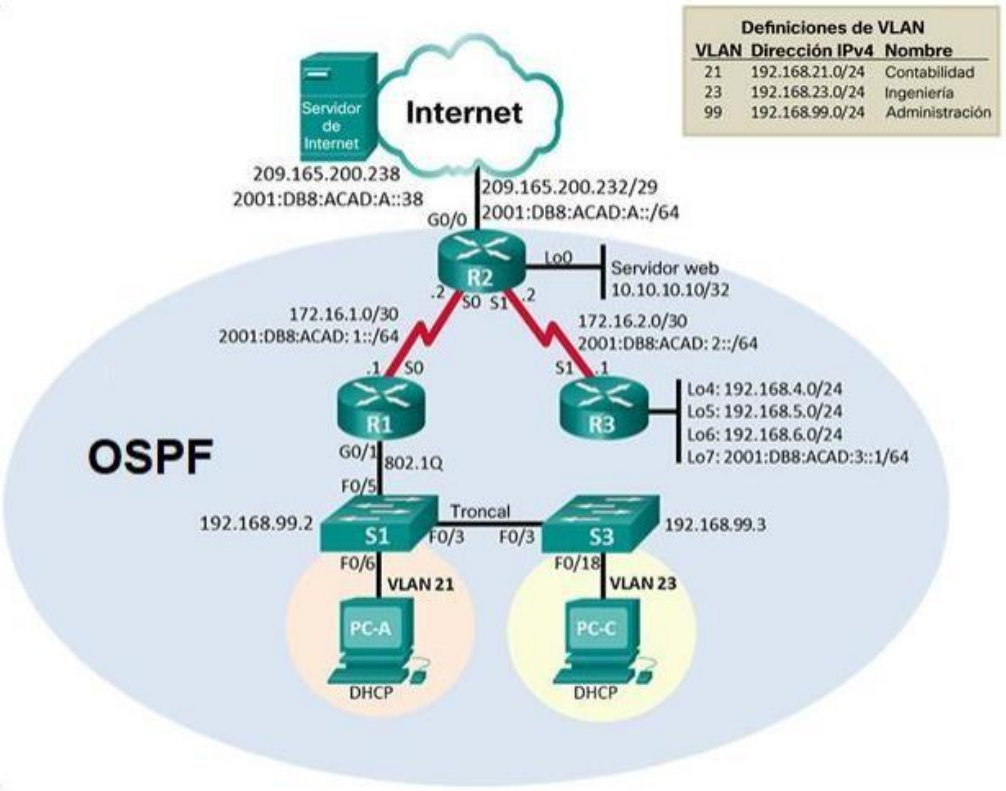
Figura 25.



ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, 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.

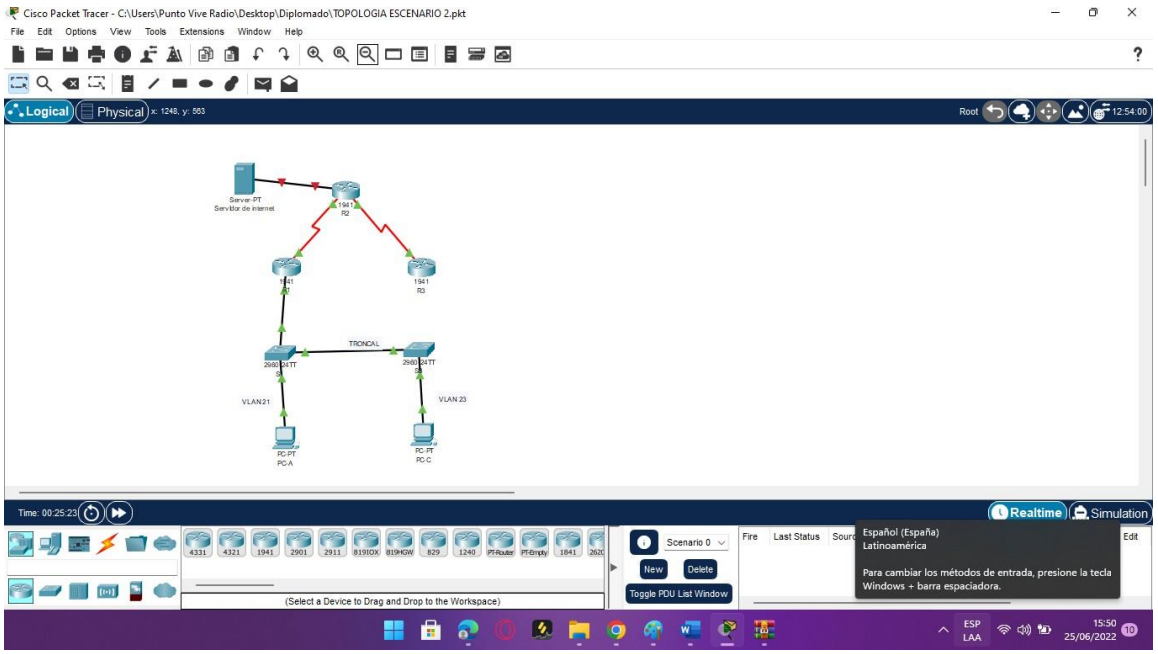
Topología



Parte 1: Inicializar dispositivos

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

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



Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	• **Router#Erase startup-config** • **Switch#Erase startup-config**
Volver a cargar todos los routers	• **Router#Reload** • **Switch#Reload**
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	• **Router#Erase startup-config** • **Router#Delete vlan.dat** • **Switch#Erase startup-config** • **Switch#Delete vlan.dat**
Volver a cargar ambos switches	• **Router# Reload** • **Switch#Reload**
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	• **Router#Show flash** • **Switch#Reload**

Para efectuar este paso, primero vamos a la pestaña CLI, allí damos enter y volvemos a presionar enter para iniciar, nos aparecerá la línea de comando router> y switch> según corresponda, esto quiere decir que los dispositivos están en usuario modo normal, y en este usuario no se puede realizar ninguna configuración. Entonces luego colocamos el comando enable para cambiar de usuario y damos 15 enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado router# y switch#, como se muestra a continuación.

- **Router> enable**
- **Router#**

- **Switch> enable**

- **Switch#**

Por medio del comando erase startup-config eliminamos los archivos y con el comando reload volverá a cargar los dispositivos.

- **Router> enable**
- **Router# erase startup-config**
- **Router# reload**

- **Switch> enable**
- **Switch# erase startup-config**
- **Switch# reload**

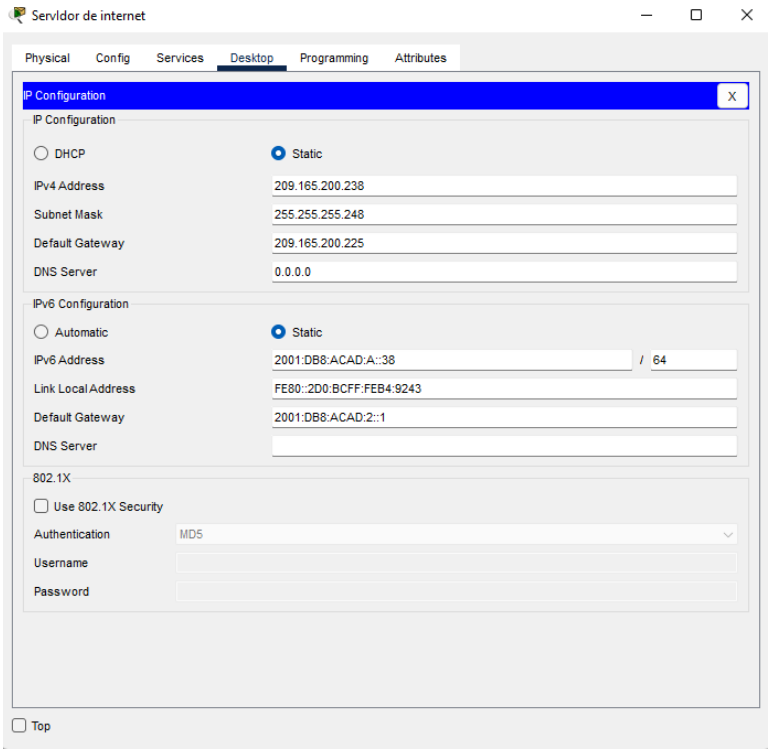
PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

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):

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	**2**001:DB8:ACAD:2::1
Gateway predeterminado IPv6	**2**001:DB8:ACAD:2::1

Figura 27 configuración del servidor de Internet



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:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R1(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)#password cisco
Contraseña de acceso Telnet	R1(config)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd $Se prohibe el acceso no autorizado$
	• R1(config)#interface s0/3/0

Interfaz S0/0/0	• R1(config-if)#ip address 172.16.1.1 255.255.255.252 • R1(config-if)#clock rate 128000 R1(config-if)#no shutdown • R1(config)#interface s0/3/0 • R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 • R1(config-if)#no shutdown
Rutas predeterminadas	• R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/0/0 • R1(config)#ipv6 route ::/0 serial s0/0/0

Nota: Todavía no configure G0/1

PASO 3: CONFIGURAR R2

Para realizar la configuración del router R2 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es R2.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.
8. Configurar la interfaz s0/3/0 y s0/3/1 en R2, según la topología y establecer la frecuencia de reloj en 128000 para todas las interfaces DCE del router.
9. Configurar la interfaz G0/0 que conecta con el PC, para la simulación de internet. además, se configurar rutas predeterminadas para ipv4 y ipv6 a través del comando ip route, las direcciones IP se muestran en la topología.
10. Configurar la Interfaz loopback o servidor web simulado

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(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)#password cisco
Contraseña de acceso Telnet	R2(config)#password cisco
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	• R2(config)#interface s0/0/0 • R2(config-if)#ip address 172.16.1.2 255.255.255.252 • R2(config-if)#clock rate 128000 • R2(config-if)#no shutdown • R2(config)#interface s0/0/0 • R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 • R2(config-if)#no shutdown
Interfaz S0/0/1	• R2(config)#interface s0/0/1 • R2(config-if)#ip address 172.16.2.2 255.255.255.252 • R2(config-if)#clock rate 12800 R2(config-if)#no shutdown • R2(config)#interface s0/3/1 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	• R2(config)#interface s0/3/1 • R2(config-if)#ip address 172.16.2.2 255.255.255.252 • R2(config-if)#clock rate 12800 • R2(config-if)#no shutdown • R2(config)#interface s0/3/1 • R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 • R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	• R2(config)#interface loopback 0 • R2(config-if)#ip address 10.10.10.10 255.255.255.255 • R2(config-if)#no shutdown

Ruta predeterminada	• R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 • R2(config)#ipv6 route ::/0 g0/0

PASO 4: CONFIGURAR R3

Para realizar la configuración del router R3 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando router> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto meramente colocamos el comando no ip domain lookup. 23
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es router, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es R3.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del router banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el router permita el acceso por vía Telnet.
8. Configurar la interfaz s0/3/1 en R3 para ipv4 y ipv6, según la topología y establecer la frecuencia de reloj en 128000 para todas las interfaces DCE del router.
9. Configurar la interfaz G0/0 que conecta con el PC, para la simulación de internet.
10. Configurar la Interfaz loopback o servidor web simulado 4,5,6 y 7, las direcciones IP se encuentran en la topologia.

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	ESPECIFICACIÓN
Desactivar la búsqueda DNS	R3(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#password cisco
Contraseña de acceso Telnet	R3(config)#password cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption

Mensaje MOTD	R3(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/1	• R3(config)#interface s0/3/1 • R3(config-if)#ip address 172.16.2.1 255.255.255.252 • R3(config-if)#clock rate 128000 • R3(config-if)#no shutdown R3(config)#interface s0/3/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 • R3(config-if)#no shutdown
Interfaz loopback 4	• R3(config)#interface loopback 4 • R3(config-if)#ip address 192.168.4.0 255.255.255.0 • R3(config-if)#no shutdown
Interfaz loopback 5	• R3(config)#interface loopback 5 • R3(config-if)#ip address 192.168.5.0 255.255.255.0 • R3(config-if)#no shutdown
Interfaz loopback 6	• R3(config)#interface loopback 6 • R3(config-if)#ip address 192.168.6.0 255.255.255.0 • R3(config-if)#no shutdown
Interfaz loopback 7	• R3(config)#interface loopback 7 • R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 • R3(config-if)#no shutdown

Rutas predeterminadas	Se configura las interfaces por defecto, rutas por las cuales se envía la información que no cuenta con una ruta conectada directamente:
	`ip classless`
	`ip route 0.0.0.0 0.0.0.0 Serial0/0/1`
	`!`
	`ip flow-export version 9`
	`!`
	`ipv6 route ::/0 Serial0/0/1`

PASO 5: CONFIGURAR S1

Para realizar la configuración del switch S1 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando switch> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto solamente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es switch, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es S1.
4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del switch banner motd y seguido el mensaje.
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el switch permita el acceso por vía Telnet.
8.

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	**S1(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)#password cisco**
Contraseña de acceso Telnet	**S1(config)#password cisco**
Cifrar las contraseñas de texto no cifrado	**S1(config)#service password-encryption**
Mensaje MOTD	**S1(config)#banner motd $Se prohibe el acceso no autorizado$**

PASO 6: CONFIGURAR EL S3

Para realizar la configuración del switch S3 se seguirán los siguientes pasos:

1. Ir a la pestaña CLI, donde nos aparecerá la línea de comando switch> colocamos el comando enable para cambiar de usuario y damos enter para pasar a un usuario con privilegios.
2. Desactivar la búsqueda de nombres de dominio, para esto solamente colocamos el comando no ip domain lookup.
3. Cambiar el nombre de usuario, en este caso su nombre por defecto es switch, lo cambiaremos por medio del comando hostname y seguido del comando se asigna el nombre que para este caso es S3.

4. Escribir el comando service password-encryption para encriptar las contraseñas, además le colocamos una contraseña secreta que no se podrá visualizar por medio del comando enable secret class.
5. Agregar un mensaje de advertencia que se mostrara al inicio de la línea de comando del switch banner motd y seguido el mensaje. 28
6. Agregar las contraseñas a las líneas de consola y línea vty por medio de los comandos line console 0 y line vty 0 4 enter password cisco, después tenemos que escribir el comando login para que acepte y aplique las contraseñas
7. Configurar las líneas de terminal virtual (vty) para que el switch permita el acceso por vía Telnet.

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3(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)#password cisco
Contraseña de acceso Telnet	S3(config)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$

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

Desde	A	Dirección IP	Resultados de ping
R1	**R2, S0/0/0**	172.16.1.2	Satisfactorio
R2	**R3, S0/0/1**	172.16..2.1	Satisfactorio
PC de Internet	**Gateway predeterminado**	209.165.200.225	Satisfactorio

Verificación de las configuraciones basicas ping desde R1 a R2

```
R1#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R1#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

VERIFICACIÓN DE LAS CONFIGURACIONES BASICAS PING DESDE R2 A R3

```
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 = 1/1/2 ms

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 = 1/4/16 ms
```

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

Paso 1: Configurar S1

Primeramente, vamos a crear las tres VLAN con su respectivo nombre, luego vamos a configurar la dirección IP de las interfaces, direcciones que podemos observar en la topología y el gateway predeterminado para cada switch. Seguidamente configuramos la interface fa0/3 y fa0/5, como troncal para que se comunique con el router y utilizamos la red nativa 1, para que la información se transmita por esta vía. También se configuran los otros puertos como puertos de acceso con el comando switchport mode access. A la interface fa0/6 se le asigna la VLAN 21, después apagamos los puertos sin usar por medio del comando no shutdown

La configuración del S1 incluye las siguientes tareas:

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 administración • S1(config-vlan)#exit
Asignar la dirección IP de administración.	• S1(config-if)#interface vlan 99 • S1(config-if)#ip address 192.168.99.2 255.255.255.0 • S1(config-if)#no shutdown
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 fa0/3 • 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)#interface fa0/5 • S1(config-if)#switchport mode trunk • S1(config-if)#switchport trunk native vlan 1 • S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	• S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 • S1(config-if-rangen)#switchport mode access
Asignar F0/6 a la VLAN 21	• S1(config-if)#interface fa0/6 • S1(config-if)#switchport mode access • S1(config-if)#switchport access vlan 21 • S1(config-if)#no shutdown
Apagar todos los puertos sin usar	S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-range)#shutdown

Tabla Indicaciones para configurar la seguridad del switch y el routing entre las vlan de S1.

PASO 2: CONFIGURAR EL S3

Se crean las tres VLAN con su respectivo nombre en el switch S3, se asignan las direcciónes IP de las VLAN y el gateway predeterminado. Seguidamente configuramos la interface fa0/3, como troncal para que se comunique con el router y utilizamos la red nativa 1, para que la información se transmita por esta

vía. También se configuran los otros puertos como puertos de acceso con el comando switchport mode access. A la interface fa0/18 se le asigna la VLAN 21 y después apagamos los puertos sin usar por medio del commando shutdown.

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	• S3(config)#vlan 21 • S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 • S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 • S3(config-vlan)#name administración • S3(config-vlan)#exit
Asignar la dirección IP de administración	• S3(config)#interface vlan 99 • 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)#interface fa0/3 • 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)#interface range fa0/2, fa0/4-24, g0/1-2 • S3(config-if)#switchport mode Access
Asignar F0/18 a la VLAN 21	• S3(config-if)#interface fa0/18 • S3(config-if)#switchport mode access • S3(config-if)#switchport access vlan 23 • S3(config-if-range)#no shutdown
Apagar todos los puertos sin usar	• S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 • S3(config-if-range)#shutdown

Paso 3: Configurar R1

En este paso se configurarán la subinterfaz 802.1Q en la interfaz g0/1, creamos los puertos virtuales para cada VLAN asignándole una dirección IP dependiendo

de estas mismas y por último se enciende la interfaz por medio del comando no shutdown.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/1.21 R1(config-subif)#description accounting LAN 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)# interface g0/1.23 • R1(config-subif)#description accounting LAN • 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)# interface g0/1.99 • R1(config-subif)#description accounting LAN • 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)# interface g0/1 R1(config-subif)#no shutdown

PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

Se utiliza el comando ping en cada uno de los dispositivos para probar la conectividad entre los dispositivos de red. Si algún ping entre los routers falla, se corregira usando los comandos show ip route, show ipv6 route, show ip interface brief y show vlan brief para detector los posibles problemas, estos comandos nos permiten verificar las configuraciones que se realizaron y las vlan que se crearon con sus respectivas direcciones IP.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 m

S3	R1, dirección VLAN 99	192.168.99.1	Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/6 ms
S1	R1, dirección VLAN 21	192.168.21.1	Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/6 ms
S3	R1, dirección VLAN 23	192.168.21.1	Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/6 ms

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:

ELEMENTO O TAREA DE CONFIGURACIÓN	ESPECIFICACIÓN
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0
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

PASO 2: CONFIGURAR OSPF EN EL R2

En este paso se configura el protocolo RIPv2 en el router R2, v2 quiere decir que se utiliza la versión 2, por medio del comando router rip entramos en el modo protocolo RIP, seguidamente colocamos la versión, después se anunciaran las redes que están conectadas directamente usando el comando network.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router rip R2(config-router)#version 2

Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 10.10.10.10 R2(config-router)#network 192.168.4.0 R2(config-router)#network 192.168.5.0 R2(config-router)#network 192.168.6.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

PASO 3: CONFIGURAR RIPV2 EN EL R3

En este paso se configura el protocolo RIPv2 en el router R3, v2 quiere decir que se utiliza la versión 2, por medio del comando router rip entramos en el modo protocolo RIP, seguidamente colocamos la versión, después se anunciaran las redes que están conectadas directamente usando el comando network. Se establecerán las interfaces LAN loopback 4,5 y 6 como pasivas, por medio del comando passive-interface y por último se desactiva la sumarizacion automática con el comando auto-summary

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
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	R3(config-router)#no auto-summary

PASO 4: VERIFICAR LA INFORMACIÓN DE RIP

Para realizar la verificación de las configuraciones que se realizaron en los router con el protocolo RIPv2 podemos utilizar el commando show ip protocols, este comando no solo nos muestra que protocolo estamos usando, sino también las rutas que anunciamos como cercanas al router y las rutas que se configuraron

como pasivas. El comando show ip route rip nos muestra solamente las rutas rip que configuramos El comando show running-config nos permite ver todas las configuraciones que se han realizado en el dispositivo.

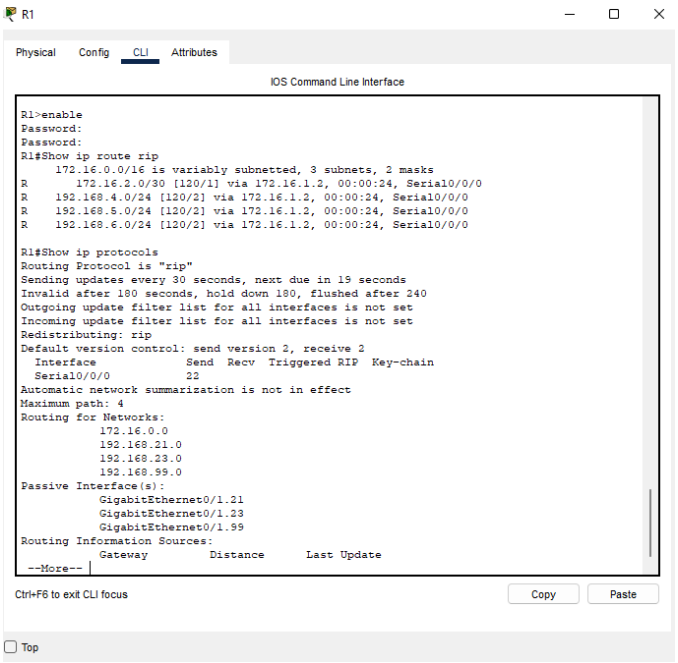
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#Show ip protocols R2#Show ip protocols R3#Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#Show ip route rip R2#Show ip route rip R3#Show ip route rip
¿Qué comando muestra la sección de OSPF de la configuración en ejecución	R1#Show run R2#Show run R3#Show run

Parte 5: Implementar DHCP y NAT para IPv4

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

R1#Show ip protocols y R1#Show ip route rip



R2#Show ip protocols

```
R2>enable
Password:
R2#Show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0           22
  Serial0/0/1           22
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
            10.0.0.0
            172.16.0.0
Passive Interface(s):
            Loopback0
Routing Information Sources:
            Gateway         Distance      Last Update
            172.16.2.1           120      00:00:01
            172.16.1.1           120      00:00:03
Distance: (default is 120)
R2#
```

Ctrl+F6 to exit CLI focus Copy Paste

R2#Show ip route rip

```
R2#Show ip route rip
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R    192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:22, Serial0/0/1
R    192.168.5.0/24 [120/1] via 172.16.2.1, 00:00:22, Serial0/0/1
R    192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:22, Serial0/0/1
R    192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:24, Serial0/0/0
R    192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:24, Serial0/0/0
R    192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:24, Serial0/0/0

R2#
```

Ctrl+F6 to exit CLI focus Copy Paste

R2#Show run

```
R2#Show run
Building configuration...

Current configuration : 2063 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
no ip cef
no ipv6 cef
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

R3#Show ip protocols

```
R3>enable
Password:
R3#Show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 24 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial0/0/1           22
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
            172.16.0.0
            192.168.4.0
            192.168.5.0
            192.168.6.0
Passive Interface(s):
            Loopback4
            Loopback5
            Loopback6
            Loopback7
Routing Information Sources:
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

R3#Show ip route rip

```
R3#Show ip route rip
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:19, Serial0/0/1
     192.168.7.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:19, Serial0/0/1
R    192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:19, Serial0/0/1
R    192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:19, Serial0/0/1


R3#
```

Ctrl+F6 to exit CLI focus Copy Paste

R3#Show run

```
R3#Show run
Building configuration...

Current configuration : 1558 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
no ip cef
ipv6 unicast-routing
 --More--
```

Ctrl+F6 to exit CLI focus Copy Paste

PARTE 5: IMPLEMENTAR DHCP Y NAT PARA IPV4

PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

Ahora configuramos el dhcp en R1, por medio del comando ip dhcp pool para la VLAN 21 y la 23, le asignamos un nombre ACCT y ENGNR, un servidor DNS con la IP 10.10.10.10, un nombre de dominio ccna-sa.com y la puerta de enlace según corresponda a la VLAN y además se guardan las primeras 20 direcciones IP para la VLAN 21 y la VLAN 23

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	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 dchp pool ACCT R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.23.1

PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

Primero se crea una base de datos local por medio del comando user, en donde webuser es el nombre de usuario, privilege 15 es decir con privilegio 15 y con una contraseña secreta cisco 12345. Luego creamos una NAT estatica con el commando ip nat inside source static con la direccion IP 10.10.10.10 y la puerta de enlace 209.165.200.229, despues asignamos la interfaz g0/1 como externa y la interfaz f0/6 como interna para la NAT estatica que se creo anteriormente.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet Tracer no procesa la configuraion HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Defina el pool de direcciones IP públicas utilizables.	R2(config)#interface gi0/1 R2(config)#ip nat outside R2(config)#interface fa0/6 R2(config)#ip nat inside
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.

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

PARTE 6: CONFIGURAR NTP

NTP es un protocolo diseñado para sincronizar los relojes de las estaciones de trabajo a través de la red, por medio de los siguientes comandos realizaremos esta configuración en los dispositivos. A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R1 y R2

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 5 de marzo de 2016, 9 a. m
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	R1#show ntp associations R1#show clock

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

Paso 1: Restringir el acceso a las líneas VTY en el R2 A continuación, se muestran los comandos tal como se escribirían en la ventana CLI del router R2, para restringir el acceso a las líneas de control de acceso.

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 standart ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	

PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

En la tabla que se muestra en este paso, observaremos algunos comandos necesarios según la necesidad que tengamos en el momento de estar realizando las configuraciones y después de terminarlas.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	#show ip access list
Restablecer los contadores de una lista de acceso	#clear ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	#show ip interface
¿Con qué comando se muestran las traducciones NAT?	#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	#clear ip nat translations

CONCLUSIONES

El desarrollo de los diferentes protocolos y rutas permitió analizar qué tan efectivos y eficientes son al momento de su aplicación en los distintos escenarios propuestos y así analizar su comportamiento al momento de su aplicación. Esto evidencio que tan eficientes son las herramientas de supervisión que utilizan estos protocolos de administración de redes al momento de la resolución de problemas.

Por otro lado, asignando seguridad a los dispositivos de red a través de comandos de línea, permitió la correcta resolución de los problemas de conectividad, evidenciando que su aplicabilidad es conveniente.

De igual forma seguir los pasos y aplicarlos según la guía configurando los dispositivos de red a través de comandos básicos demuestra su eficiencia. Así mismo estas prácticas permiten que al momento que se presenten en escenarios reales sea más fácil resolver los problemas de los entornos reales.

BIBLIOGRAFIA

CISCO. "Exploración de la red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

CISCO. " Configuración de un sistema operativo de red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

CISCO. "Protocolos y comunicaciones de red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. " Acceso a la red. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. "Ethernet: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. "Capa de red: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. " División de redesIP en subredes: Fundamentos de Networking.". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. "Capa de Transporte: Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. "Capa de Aplicación. Fundamentos de Networking". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. "Conceptos de Routing: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

CISCO. " Routing Estático: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. " Routing Dinámico: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

UNAD "Principios de Enrutamiento [OVA]". {En línea}. {28 de noviembre de 2021} Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. " Configuración del Switch: Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. "VLANs. Principios de Enrutamiento y Conmutación. {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. "Listas de control de acceso. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. " DHCP. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. " NAT para IPv4. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

CISCO. " Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación". {En línea}. {28 de noviembre de 2021} Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10