

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

FERNANDO TRUJILLO

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

FERNANDO TRUJILLO

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

DIRECTOR:  
HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA SISTEMAS  
LA PLATA HUILA

NOTA DE ACEPTACION

---

---

---

---

---

---

Firma presidente del Jurado.

---

Firma del Jurado

---

Firma del Jurado

La plata Huila, 25 de junio de 2022

## AGRADECIMIENTOS.

Primero que todo le agradezco infinitamente a Dios por permitirme superarme constantemente, Agradezco a mi familia, a mis padres ya que gracias al apoyo que me han brindado a lo largo de toda mi carrera fue posible llegar al punto en el que ahora estoy, agradezco a la Universidad Nacional Abierta y a Distancia UNAD institución que me permitió formarme como profesional gracias al apoyo de todo sus docentes, directivos y personal.

## TABLA DE CONTENIDO

TABLA DE FIGURAS.....	7
Lista de Tablas.....	8
GLOSARIO.....	9
RESUMEN.....	11
ABSTRACT .....	12
INTRODUCCIÓN.....	13
DESARROLLO .....	14
1. DESARROLLO ESCENARIO 1.....	14
Objetivos.....	14
Aspectos básicos/situación.....	14
1.1 Construcción de la Red.....	15
1.2 Desarrolle el esquema de direccionamiento IP.....	15
1.2.1 Subneteo del rango IP: .....	15
1.3 Configure aspectos básicos .....	17
1.3.1 Configuración para R1 incluyen las siguientes:.....	17
Comandos empleados para configurar el R1: .....	19
1.3.2 Proceso de configuración de S1: .....	19
1.3.3 Configurar los equipos PC.....	22
1.4 Prueba de conectividad.....	24
2. DESARROLLO ESCENARIO 2.....	27
Topología.....	27
2.1 Inicializar dispositivos.....	27
2.1.1 Inicializar y volver a cargar los routers y los switches.....	27
2.2 Configurar los parámetros básicos de los dispositivos.....	28
2.3 Configurar la computadora de Internet.....	28
2.4 Configuración de R1.....	30
2.5 Configuración de R2.....	32
2.6 Configuración de R3.....	36
2.7 Configuración de S1.....	39
2.8 Configuración de S3.....	40
2.9 Verificar la conectividad de la red.....	40
3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN.....	42
3.1 Configuración VLAN, routing y seguridad en S1.....	42
3.2 Configuración VLAN, routing y seguridad en S3.....	43
3.3 Configuración de subinterfaces y encapsulación en R1.....	44
3.4 Verificar la conectividad de la red.....	46
4. Configurar el protocolo de routing dinámico OSPF .....	47
4.1 Configurar OSPF en el R1 .....	47
4.2 Configurar OSPF en el R2 .....	49
4.3 Configurar OSPFv3 en el R3.....	51
4.4 Verificar la información de OSPF.....	52

5. Implementar DHCP y NAT para IPv4 .....	53
5.1 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 .....	53
5.2 Configurar la NAT estática y dinámica en el R2 .....	55
5.3 Verificar el protocolo DHCP y la NAT estática.....	58
6. Configurar NTP .....	61
7. Configurar y verificar las listas de control de acceso (ACL) .....	62
7.1 Restringir el acceso a las líneas VTY en el R2.....	62
• TELNET desde R1 a R2.....	63
7.2 Introducir el comando de CLI adecuado que se necesita para mostrarlo siguiente.	63
CONCLUSIONES.....	65
BIBLIOGRAFIA.....	66
ANEXOS.....	67

## TABLA DE FIGURAS

	pág.
ESCENARIO 1	
Figura 1: Topología escenario 1	14
Figura 2: Topología en Packet Tracer.	16
Figura 3 Topología ESCENARIO 1.	16
Figura 4: Configuración PC-A	22
Figura 5: Configuración PC-B	23
Figura 6: MAC PC-A	24
Figura 7: Dirección MAC - PCB	24
Figura 8: Comando PING desde PCB hacia los diferentes puntos de la red.	25
Figura 9: Topología prueba de conectividad.	26
Figura 10: Comando PING desde PCA hacia los diferentes puntos de la	26
ESCENARIO 2	
Figura 1 - TOPOLOGIA ESCENARIO 2.	27
Figura 2 - show flash.	28
Figura 3 - configuración PC-internet.	29
Figura 4 - configuración del servidor WEB.	36
Figura 5 – PING desde R1.	41
Figura 6 – PING desde R2.	41
Figura 7 – PING desde S1.	46
Figura 8 – PING desde S1.	47
Figura 9 - Configurar OSPF en el R1	49
Figura 10 - Configurar OSPF en el R2	50
Figura 11 - Configurar OSPFv3 en el R3	51
Figura 12 – show ip protocols	52
Figura 13 - show ip route OSPF.	53
Figura 14 - show ip OSPF neighbor	53
Figura 15 - Implementar DHCP y NAT para IPv4	55
Figura 16 - Configurar la NAT estática y dinámica en el R2	58
Figura 17 - verificación de DHCP.	60
Figura 18 - verificación servicio WEB.	61
Figura 19 - TELNET desde R1 a R2	63
Figura 20 - verificación de NAT.	64

## LISTA DE TABLAS

	pág.
ESCENARIO 1	14
Tabla 1: Asignación de subredes.	15
Tabla 2: Configuración básica y asignación de direcciones IP.	16
Tabla 3: Configuración básica R1.	17
Tabla 4: Configuración básica S1.	20
Tabla 5: Configuración PC-A.	22
Tabla 6: Configuración PC-B	23
ESCENARIO 2	29
Tabla 1 – Configuración PC – internet.	29
Tabla 2 – Configuración R1.	30
Tabla 3 – Configuración R2.	32
Tabla 4 – Configuración R3.	36
Tabla 5 – Configuración S1.	39
Tabla 6 – Configuración S3.	40
Tabla 7 – Prueba de conectividad.	41
Tabla 8 – Configuración interfaces S1	42
Tabla 9 – Configuración interfaces S3	43
Tabla 10 – Configuración interfaces R1	44
Tabla 11 – Prueba de conectividad desde los ROUTERS	46
Tabla 12 – Configuración de OSPF en R1	47
Tabla 13 – Configuración de OSPF en R2	49
Tabla 14 – Configuración de OSPF en R3	51
Tabla 15 – Comandos de verificación de OSPF.	52
Tabla 16 – Configuración de DHCP.	53
Tabla 17 – Configuración NAT estático Y dinámico.	55
Tabla 18 – Verificación de DHCP y NAT.	58
Tabla 19 – NTP	62
Tabla 20 – Restringir el acceso a las líneas VTY en el R2	62
Tabla 21 – Comando SHOW.	63



## GLOSARIO

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

**IOS:** Son las siglas de Internetwork Operating System, (Sistema Operativo de Interconexión de Redes) sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

**LAN red de área local (del inglés Local Área Network):** Es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir Recursos e intercambiar datos y aplicaciones.

**MODELO OSI:** Este es un modelo que sirve como estándar de referencia que fija los modelos de las comunicaciones; inicialmente fue creado por la ISO y actualmente se mantiene ya que permite estandarizar la comunicación global de internet y también de área local por medio del establecimiento de protocolos de comunicación entre equipos de cómputo, en este sentido todos los paquetes enviados atraviesan las 7 capas de este modelo OSI.

**NAT:** La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

**OSPF:** protocolo Primero la ruta más corta (OSPF = Open Shortest Path First – Protocolo abierto de los enlaces) es uno de los protocolos del estado-enlace más importantes. Es un protocolo estándar descrito en el RFC 2328 y la versión para IPv6 se publicó en el RFC 2740. Usa el algoritmo SPF para calcular el costo más Bajo hasta un destino. Las actualizaciones de enrutamiento producen tráfico cuando ocurren cambios en la topología de la red.

**PROTOCOLO DE RED:** Es el conjunto de reglas estándar que se utilizan para la comunicación en redes de computadores de cualquier tipo, ya sean LAN, WAN, etc. Por los que se establece una semántica y sintaxis a seguir para que sea más fácil de entender a la misma vez que funciona de la manera más óptima.

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

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

**WAN:** Una Red de Área Amplia (Wide Área Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

## RESUMEN

El presente diplomado de CISCO CCNA se desarrolla 2 escenarios, el primero se busca a través del desarrollo de una red pequeña y gracias a la cual vamos a aplicar nuestros conocimientos en su configuración, debemos indicar los diferentes pasos, los comandos que se ejecutan, los protocolos que se van a configurar y además de esto debemos realizar la puesta en marcha de la misma empleando el simulador de redes de cisco Packet Tracer, este simulador es una excelente herramienta para nosotros como estudiantes, pues me permite armar la topología indicada, configurar cada uno de los dispositivos que intervienen y poder verificar el correcto funcionamiento. Para este primer caso el direccionamiento que se va a emplear es el direccionamiento IPV4 aplicando VLSM con el fin de ajustar el mismo a las necesidades reales de la organización y de esta manera no generar desperdicios innecesarios. Para el desarrollo del escenario 2 la estructura del mismo, su topología y los comandos que se van a configurar son mucho más complejos, vamos a profundizar mucho más esto con el fin de aplicar todo lo aprendido a lo largo de este diplomado. Para el direccionamiento IP, se nos solicita que configuremos tanto IPV4 como IPV6, parte de la asignación de direcciones se realizará empleando DHCP, se configurará rutas estáticas, configuraremos VLAN con el fin de organizar mucho mejor nuestra red y evitar conflictos dentro de la misma, configuraremos todo lo relacionado con la seguridad de nuestra red para poder mantener la integridad de los diferentes dispositivos.

Palabras Clave: CISCO, CCNA, IPV6, VLANS, DCHP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

This CISCO CCNA diploma develops 2 scenarios, the first is sought through the development of a small network and thanks to which we are going to apply our knowledge in its configuration, we must indicate the different steps, the commands that are executed, the protocols that are going to be configured and in addition to this we must carry out the start-up of it using the cisco Packet Tracer network simulator, this simulator is an excellent tool for us as students, since it allows me to put together the indicated topology, configure each one of the devices involved and to be able to verify correct operation. For this first case, the addressing that is going to be used is the IPV4 addressing applying VLSM in order to adjust it to the real needs of the organization and thus not generate unnecessary waste. For the development of scenario 2, its structure, its topology and the commands that are going to be configured are much more complex, we are going to deepen this much more in order to apply everything learned throughout this course. For IP addressing, we are asked to configure both IPV4 and IPV6, part of the address assignment will be done using DHCP, static routes will be configured, VLANs will be configured in order to better organize our network and avoid conflicts within it, We will configure everything related to the security of our network in order to maintain the integrity of the different devices.

Keywords: CISCO, CCNA, IPV6, VLANS, DCHP, Switching, Routing, Networks, Electronics.

## INTRODUCCIÓN

Desde hace muchos años atrás el proceso de comunicación se ha convertido en algo indispensable para nuestra sociedad, buscando que la misma sea mucho mas eficiente y en tiempo real; inicialmente gran parte de este desarrollo a tenido sus inicios con fines militares, gracias a esto las telecomunicaciones avanzaron muchísimo y ya no solo dentro de este campo, sino que se han convertido en parte esencial dentro de nuestras vidas. No olvidemos que cada avance debe ir de la mano con muchos otros aspectos, para nuestro caso el Hardware, la electrónica igualmente a permitido que los avances sean posibles.

Como vemos a nuestro alrededor las formas en que se transmite la información ha cambiado mucho, son numerosas las formas en las cuales estas se puedes lograr y llegar a diferentes puntos ya no importando la distancia entre los mismo, los medios mas comunes se encuentran el microondas, satelital, ondas electromagnéticas, o por fibras de vidrio, y todos estos aplican el modelo OSI como estándar para la transmisión de datos entre dispositivos.

Para nuestro caso vamos a realizar la configuración de 2 escenarios, en el primer caso se va a configurar una red LAN y para el segundo una red WAN las cuales me van a permitir conectar los diferentes dispositivos indicados dentro de la topología, emplearemos para esto tanto direccionamiento IPV4 como IPV6 para la configuración de las diferentes interfaces tanto de los PC, Routers, Switches. Vamos a crear una serie de VLANS y de esta manera poder tener un control adecuado de las diferentes dependencias. Por último, es vital configurar todo lo que tiene que ver con la seguridad, agregando y configurando aspectos como contraseñas seguras que me permitan mantener la integridad de cada uno de los dispositivos de la red y de la red en general logrando la funcionalidad de la organización.

## DESARROLLO

### 1. DESARROLLO ESCENARIO 1.

A continuación, se indica el Escenario Número 1 que hace parte de la prueba de habilidades.

Escenario 1

Topología

Figura 1: Topología escenario 1



Fuente: Autoría propia.

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

### Objetivos

- Parte 1: Construir en el simulador la Red
- Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
- Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
- Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
- Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

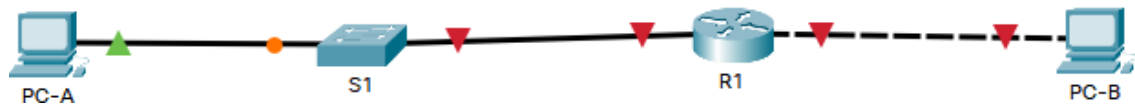
### Aspectos básicos/situación

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

## 1.1 Construcción de la Red.

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

Figura 2: Topología en Packet Tracer.



Fuente: Autoría propia:

## 1.2 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 tablade direccionamiento.

Cada estudiante tomará el direccionamiento **192.168.XX.0** donde X corresponde a los últimos dos dígitos desu cédula.

Para mi caso la dirección IP que voy a utilizar es la siguiente:

192.168.**38**.0

Con esta dirección se va a aplicar VLSM y de esta manera adaptar cada uno de los rangos a las necesidades reales del mismo, logrando que el desperdicio de direcciones IP sea mínimo.

### 1.2.1 Subneteo del rango IP:

Lo primero que debemos hacer en el caso de que conocemos la TOPOLOGÍA con los requisitos de cada una de las subredes es proceder a subnetear el rango asignado, el mismo nos queda de la siguiente manera:

Como vemos en la descripción del escenario la red está formada por 2 subredes, entonces los rangos quedan estipulados a continuación:

Tabla 1: asignación de subredes.

RED	N° IP	DIR RED	MASC	/	1RE IP	BROADCAST	N° HOST
LAN 1	100	192.168.38.0	255.255.255.128	25	192.168.38.1	192.168.36.127	126
LAN 2	50	192.168.38.128	255.255.255.192	26	192.168.38.129	192.168.38.191	62

Como ya conocemos los rangos IP para cada una de las subredes podemos proceder a realizar la asignación de la IP correspondiente a cada una de las interfaces que intervienen, este queda como se indica a continuación:

Figura 3 Topología ESCENARIO 1.



Fuente: Autoría propia.

Procedemos a realizar la asignación IP a cada interface y a realizar las primeras configuraciones a cada uno de los dispositivos.

#### Tabla de direccionamiento

Tabla 2: configuración básica y asignación de direcciones IP.

Item	Requerimiento
Dirección de Red	192.168. <b>38</b> .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  Int g0/0/1 Ip address 192.168.38.1 255.255.255.128
R1 G0/0/0	Primera dirección de host de la subred LAN2  Int g0/0/0 Ip address 192.168.38.129 255.255.255.192
S1 SVI	Segunda dirección de host de la subred LAN1  Int vlan 1 Ip address 192.168.38.2 255.255.255.128



PC-A	Última dirección de host de la subred LAN1 IP: 192.168.38.126 Mask: 255.255.255.128
PC-B	Última dirección de host de la subred LAN2 IP: 192.168.38.190 Mask: 255.255.255.192

### 1.3 Configure aspectos básicos

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

#### 1.3.1 Configuración para R1 incluyen las siguientes:

Como siguiente paso procedemos a configurar con los comandos básicos R1, nombre, desactivas búsqueda DNS, contraseñas, dominios, mensajes y las direcciones IP de las diferentes interfaces, el proceso o comandos a emplear se muestra a continuación:

*Tabla 3: configuración básica R1.*

Tarea	Especificación
Desactivar la búsqueda DNS	De esta manera conservamos recursos de nuestros dispositivos, este comando es aplicado en el router R1.  No ip domain lookup
Nombre del router	Esto se hace con el fin de identificar de manera sencilla cada uno de los dispositivos.  hostname R1
Nombre de dominio	ccna-lab.com  ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXECprivilegiado	Debemos cifrar nuestras contraseñas: ciscoenpass  enable secret ciscoenpass
Contraseña de acceso a la consola	Recordemos que el puerto de consola es un puerto físico que cualquier persona

	<p>puede acceder solo con conectar un cable, es por esto que lo debemos proteger configurando una contraseña, para nuestro caso: ciscoconpass</p> <pre>line console 0 password ciscoconnpass login</pre>
Establecer la longitud mínima para las contraseñas	<p>Configuramos el dispositivo con el fin de que cuando configuremos las contraseñas estas tengan como mínimo 10 caracteres:</p> <pre>security password min-length 10</pre>
Crear un usuario administrativo en la base de datos local	<p>Nombre de usuario: <b>admin</b> Password: <b>admin1pass</b></p> <pre>username admin secret admin1pass</pre>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	<p>Procedemos a configurar las líneas vty 0 15</p> <pre>line vty 0 15 login local</pre>
Configurar VTY solo aceptando SSH	<pre>transport input ssh login</pre>
Cifrar las contraseñas de texto no cifrado	<p>Damos seguridad a nuestras contraseñas encriptando las mismas.</p> <pre>Service password-encryption</pre>
Configure un MOTD Banner	<p>Este mensaje aparece cada vez que ingresamos a un dispositivo, es un mensaje persuasivo.</p> <pre>banner motd % SOLO SE PERMITE EL ACCESO DE FERNANDO TRUJILLO%</pre>
Configurar interfaz G0/0/0	<p>Establezca la descripción Establece la dirección IPv4. Activar la interfaz.</p> <pre>Config t Int g0/0/0 Ip address 192.168.36.129 255.255.255.192</pre>
Configurar interfaz G0/0/1	<p>Establezca la descripción Establece la dirección IPv4. Activar la interfaz.</p>

	Configure terminal Interface g0/0/01 Ip address 192.168.36.1 255.255.255.128
Generar una clave de cifrado RSA	Módulo de 1024 bits  crypto key generate rsa general-keys modulus 1024

### Comandos empleados para configurar el R1:

```

Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#username admin secret admin1pass
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#banner motd%SOLO SE PERMITE EL ACCESO DE FERNANDO
TRUJILLO%
R1(config)#do wr
R1(config)#int g0/0/1
R1(config-if)#ip address 192.168.38.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#int g0/0/0
R1(config-if)#ip address 192.168.38.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com
R1(config)#

```

### 1.3.2 Proceso de configuración de S1:

*Tabla 4: Configuración básica S1.*

Tarea	Especificación
Desactivar la búsqueda DNS.	<p>Debemos desactivar la búsqueda DNS de esta manera ahorramos recursos:</p> <p>No ip domain lookup</p>
Nombre del switch	<p>Agregamos el nombre a nuestro dispositivo S1 con el fin de poderlo identificar, por lo general en redes más grandes se emplean nombres más extensos para identificarlos con seguridad.</p> <p>hostname S1</p>
Nombre de dominio	<p><b>ccna-lab.com</b></p> <p>ip domain-name ccna-lab.com</p>
Contraseña cifrada para el modo EXEC privilegiado	<p>Creamos la contraseña de EXEC privilegiado y la ciframos Ciscoenpass</p> <p>enable secret ciscoenpass</p>
Contraseña de acceso a la consola	<p><b>Ciscoconpass</b></p> <p>line console 0 password ciscoconpass login</p>
Crear un usuario administrativo en la base de datos local	<p>Nombre de usuario: <b>admin</b> Password: <b>admin1pass</b></p> <p>username admin secret admin1pass</p>
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	<p>line vty 0 15 login local</p>
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	<p>transport input ssh</p>
Cifrar las contraseñas de texto no cifrado	<p>Este comando nos sirve para cifrar todas las contraseñas que aún no lo han hecho.</p>

	Service password-encryption
Configurar un MOTD Banner	Configuramos el mensaje que aparece en el dispositivo cuando ingresamos al mismo:  banner motd % SOLO SE PERMITE EL ACCESO DE FERNANDO TRUJILLO%
Generar una clave de cifrado RSA	<b>Módulo de 1024 bits</b>  crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento  int vlan 1 description subnet A ip address 192.168.38.2 255.255.255.128
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.  ip default-gateway 192.168.38.1

Procedemos a realizar la configuración básica del dispositivo S1, tal como se indica en la tabla anterior:

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
```

```

S1(config)#service password-encryption
S1(config)#banner motd % SOLO SE PERMITE EL ACCESO DE FERNANDO TRUJILLO%
S1(config)#crypto key generate rsa general-keys modulus 1024

```

En esta sección procedemos a configurar las interfaces que hacen parte de S1:

```

S1(config)#int vlan 1
S1(config-if)#description subnet A
S1(config-if)#ip address 192.168.10.2 255.255.255.128
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#do wr
S1(config)#

```

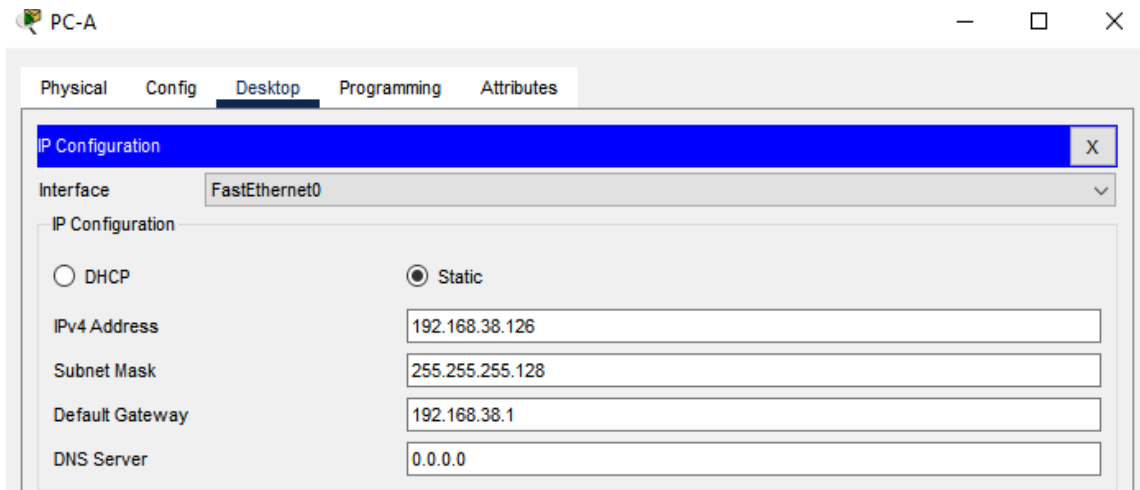
### 1.3.3 Configurar los equipos PC.

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**.

Tabla 5: configuración PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	0001.C7BC.87ED
Dirección IP	192.168.38.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.38.1

Figura 4: configuración PC-A

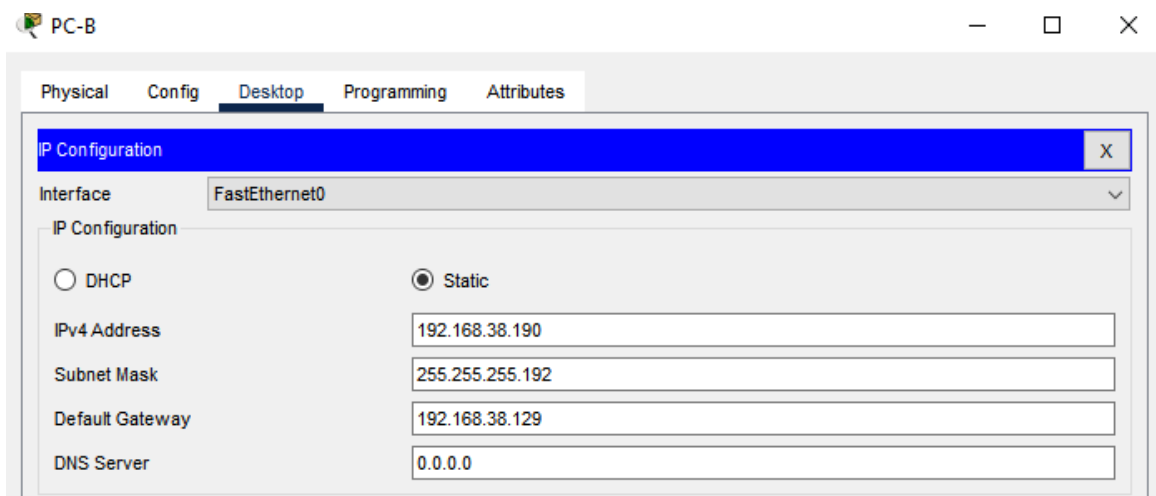


Fuente: Autoría propia

Tabla 6: configuración PC-B

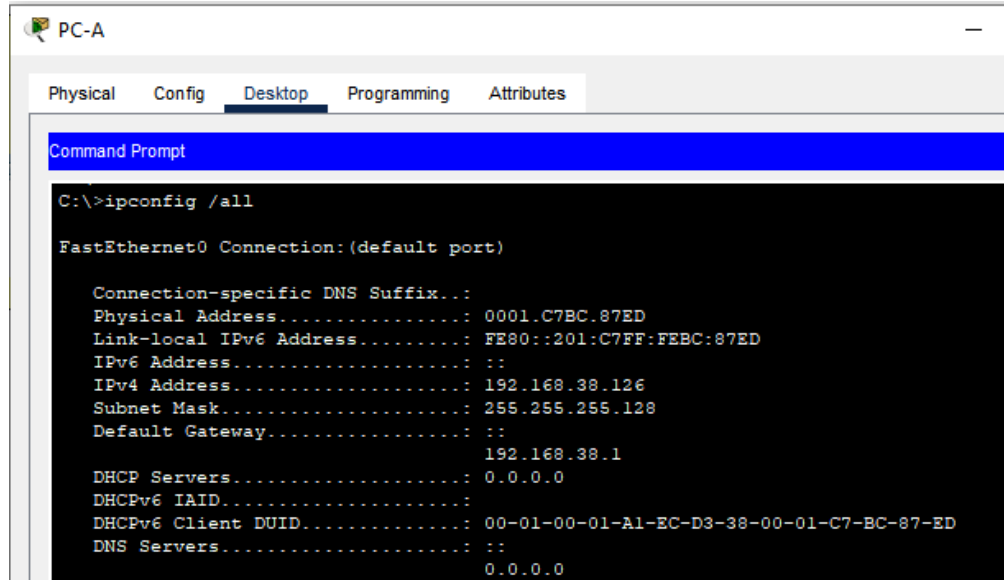
PC-B Network Configuration	
Descripción	PC-B
Dirección física	00D0.BAB6.A96B
Dirección IP	192.168.38.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.38.129

Figura 5: Configuración PC-B



Fuente: Autoría propia

Figura 6: MAC PC-A



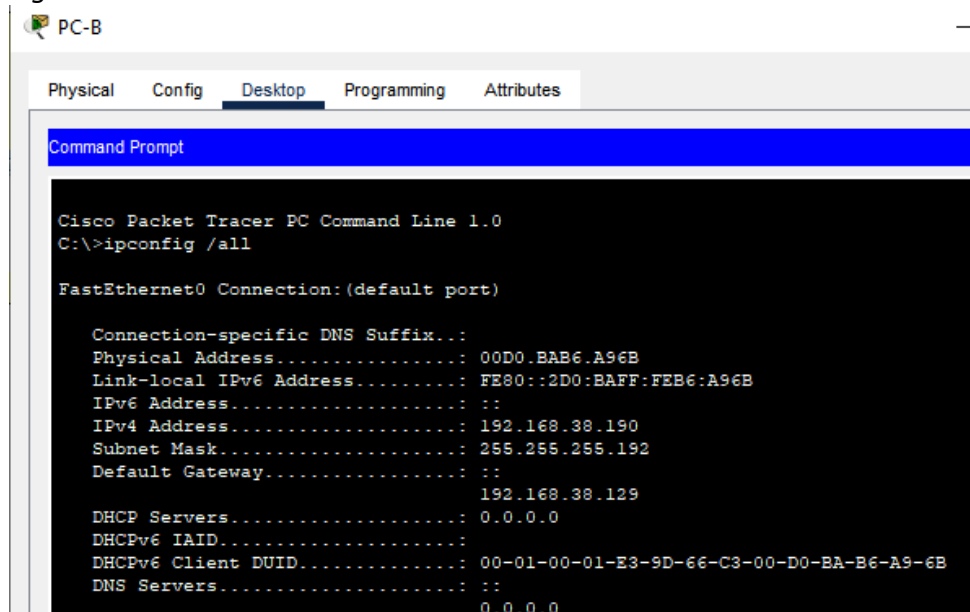
```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0001.C7BC.87ED
Link-local IPv6 Address.....: FE80::201:C7FF:FEBC:87ED
IPv6 Address.....: ::
IPv4 Address.....: 192.168.38.126
Subnet Mask.....: 255.255.255.128
Default Gateway.....: ::
                                192.168.38.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-A1-EC-D3-38-00-01-C7-BC-87-ED
DNS Servers.....: ::
                                0.0.0.0
```

Fuente: Autoría propia.

Figura 7: dirección MAC - PCB



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 00D0.BAB6.A96B
Link-local IPv6 Address.....: FE80::2D0:BAFF:FE86:A96B
IPv6 Address.....: ::
IPv4 Address.....: 192.168.38.190
Subnet Mask.....: 255.255.255.192
Default Gateway.....: ::
                                192.168.38.129
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-E3-9D-66-C3-00-D0-BA-B6-A9-6B
DNS Servers.....: ::
                                0.0.0.0
```

Fuente: Autoría propia.

#### 1.4 Prueba de conectividad.

Ya en esta parte solo me queda proceder a verificar si los pasos hechos hasta el momento son adecuados.

- Desde PCA hacia los diferentes puertos de la red.



- Procedemos a realizar la verificación de lo hecho hasta el momento, para nuestro caso vamos a emplear el comando PING desde PCB hacia los diferentes puntos de la red.

*Figura 8: Comando PING desde PCB hacia los diferentes puntos de la red.*

```
C:\>ping 192.168.38.129

Pinging 192.168.38.129 with 32 bytes of data:

Reply from 192.168.38.129: bytes=32 time<1ms TTL=255
Reply from 192.168.38.129: bytes=32 time<1ms TTL=255
Reply from 192.168.38.129: bytes=32 time=7ms TTL=255
Reply from 192.168.38.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.38.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>ping 192.168.38.1

Pinging 192.168.38.1 with 32 bytes of data:

Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Reply from 192.168.38.1: bytes=32 time=1ms TTL=255
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.38.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.38.126

Pinging 192.168.38.126 with 32 bytes of data:

Reply from 192.168.38.126: bytes=32 time=10ms TTL=128
Reply from 192.168.38.126: bytes=32 time=8ms TTL=128
Reply from 192.168.38.126: bytes=32 time=6ms TTL=128
Reply from 192.168.38.126: bytes=32 time=10ms TTL=128

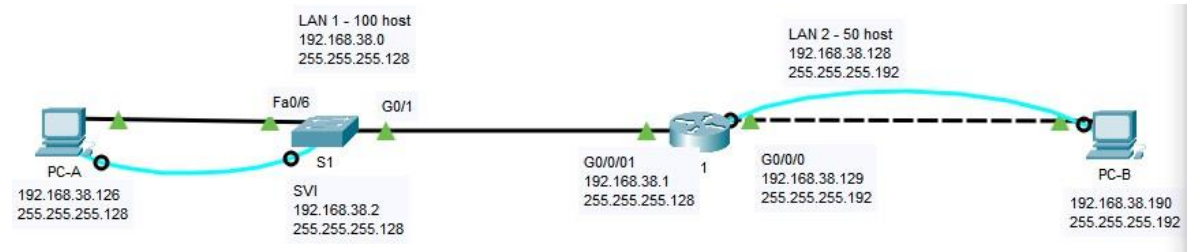
Ping statistics for 192.168.38.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 10ms, Average = 8ms

C:\>
```

*Fuente: Autoría propia.*

## Prueba de conectividad desde PCA

Figura 9: Topología prueba de conectividad.



Fuente: Autoría propia.

Figura 10: Comando PING desde PCA hacia los diferentes puntos de la red.

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.38.1
Pinging 192.168.38.1 with 32 bytes of data:
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Reply from 192.168.38.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.38.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.38.129
Pinging 192.168.38.129 with 32 bytes of data:
Reply from 192.168.38.129: bytes=32 time<1ms TTL=255
Reply from 192.168.38.129: bytes=32 time<1ms TTL=255
Reply from 192.168.38.129: bytes=32 time<1ms TTL=255
Reply from 192.168.38.129: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.38.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.38.190
Pinging 192.168.38.190 with 32 bytes of data:
Request timed out.
Reply from 192.168.38.190: bytes=32 time<1ms TTL=127
Reply from 192.168.38.190: bytes=32 time<1ms TTL=127
Reply from 192.168.38.190: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.38.190:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

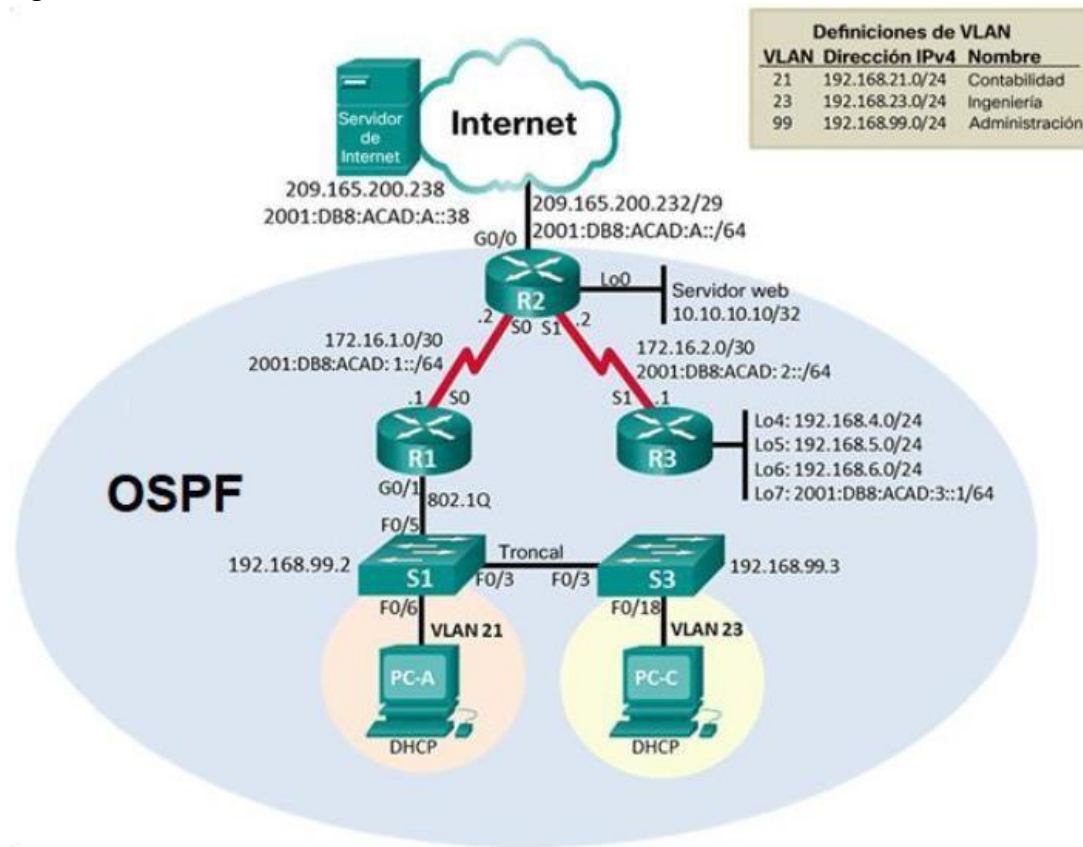
Fuente: Autoría propia.

## 2. DESARROLLO 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

Figura 1 - TOPOLOGIA ESCENARIO 2.



Fuente: CISCO.

### 2.1 Inicializar dispositivos

#### 2.1.1 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	Debemos asegurarnos que no exista algún tipo de configuración en el dispositivo que nos cree algún tipo de conflicto dentro del mismo con la nueva configuración.  erase startup-config
Volver a cargar todos los routers	Luego de eliminar posible configuración debemos proceder a reiniciar el dispositivo.:  Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Eliminamos la Base de Datos de las VLAN.  erase startup-config delete vlan.dat
Volver a cargar ambos switches	Reiniciamos el dispositivo.  Reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Procedemos a verificar que la base de datos ya no exista.  show flash

Procedemos ahora a verificar lo hecho hasta el momento..

*Figura 2 - show flash.*

```
Switch#show flash
Directory of flash:/

 1  -rw-      4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin

64016384 bytes total (59601463 bytes free)
Switch#
```

*Fuente: Autoría propia*

## 2.2 Configurar los parámetros básicos de los dispositivos

## 2.3 Configurar la computadora de Internet

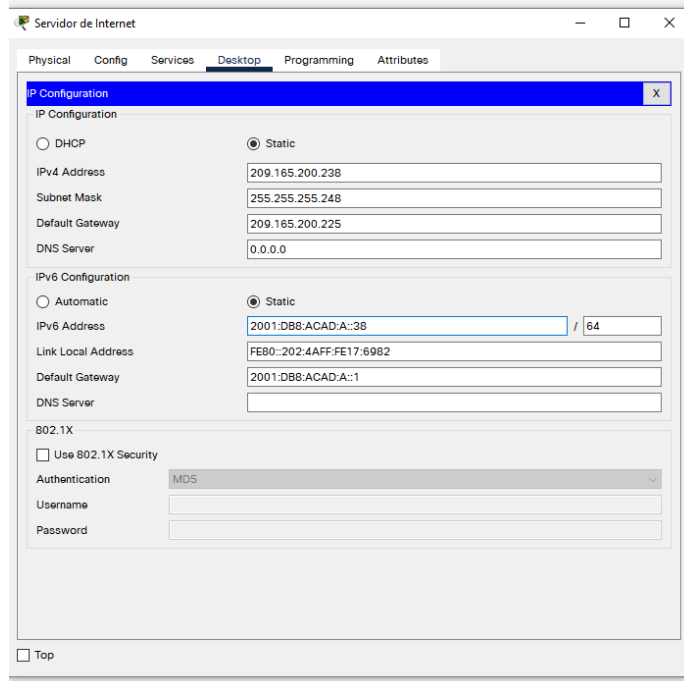
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

- Como podemos observar en la topología que se nos suministra, las direcciones IP ya han sido asignadas con anterioridad, ya solo nos queda proceder a configurar cada dispositivo:

*Tabla 1 – configuración PC – internet.*

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

*Figura 3 - configuración PC-internet.*



*Fuente: Autoría propia.*

**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.

## 2.4 Configuración de R1

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 2 – configuración R1.*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Desactivamos la búsqueda DNS, de esta manera logramos ahorrar recursos.  No ip domain lookup
Nombre del router	Debemos identificar de forma única cada uno de los dispositivos que intervienen.  Hostname R1
Contraseña de exec privilegiado cifrada	Configuramos nuestras contraseñas.  Enable secret class
Contraseña de acceso a la consola	Debemos configurar esta contraseña ya que ez el puenrto física que puede tener acceso cualquier persona.  Line console 0 Password cisco Login
Contraseña de acceso Telnet	Debemos configurar l contraseña parapoder tener acceso por medio de TELNET.  Line vty 0 4 Password cisco Login

Cifrar las contraseñas de texto no cifrado	<p>Las contraseñas se almacenan y se transfieren empleando texto cifrado evitando de esta manera que sean capturados facilmente los datos.</p> <p>Service password-encryption</p>
Mensaje MOTD	<p>Este mensaje es creado con el fin de persuadir a las personas sobre las consecuencias que podrían tener en el caso de que causen algún tipo de problemas</p> <p>Banner motd % SOLO SE PERMITE ACCESO A FERNANDO TRUJILLO%</p>
Interfaz S0/0/0	<p>Establezca la descripción  Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones  Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones  Establecer la frecuencia de reloj en 128000  Activar la interfaz</p> <p>Interface serial 0/0/0  Description connection to R2  Ip address 172,.16.1.1 255.255.255.252  Ipv6 address 2001:DB8:ACAD:1::1/64</p>
Rutas predeterminadas	<p>Configurar una ruta IPv4 predeterminada de S0/0/0  Configurar una ruta IPv6 predeterminada de S0/0/0</p> <p>Ip route 0.0.0.0 0.0.0.0 serial0/0/0  Ipv6 route ::/0 serial 0/0/0</p>

**Nota:** Todavía no configure G0/1.

## 2.5 Configuración de R2.

Continuando en este proceso procedemos a realizar las diferentes configuraciones de R2 siguiendo las siguientes indicaciones.

*Tabla 3 – configuración R2.*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Desactivamos con el fin de evitar el consume de recursos innecesarios.  No ip domain lookup
Nombre del router	Agregamos un nombre con el fin de que lo podamos identificar fácilmente.  Hostname R2
Contraseña de exec privilegiado cifrada	Configuramos este dispositivo con una contraseña. De esta manera aseguramos su estabilidad:  Enable secret class
Contraseña de acceso a la consola	Recordemos que este es un puerto físico, por consiguiente si alguien tiene acceso a los equipos puede estar realizando algún tipo de modificación que perjudique el funcionamiento del mismo.  Line console 0 Password cisco Login



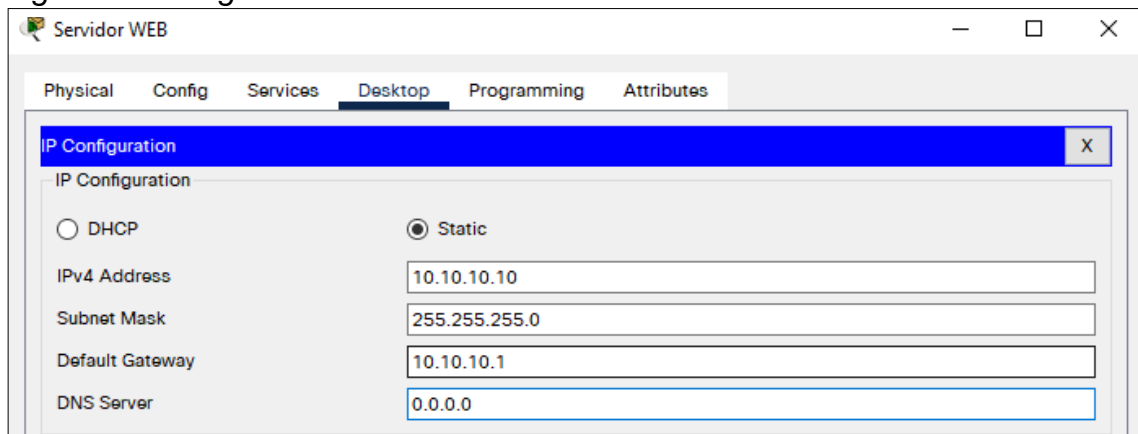
<p>Contraseña de acceso Telnet</p>	<p>Creamos las contraseñas de las líneas virtuales VTY que me permitirán el acceso remoto mediante TELNET:</p> <pre>Line vty 0 4 Password cisco Login</pre>
<p>Cifrar las contraseñas de texto no cifrado</p>	<p>Debemos proceder a encriptar las contraseñas:</p> <pre>Service password-encryption</pre>
<p>Habilitar el servidor HTTP</p>	<pre>ip http server</pre> <p>como este comando no es soportado por el simulador, se precede a instalar un servidor que haga el mismo proceso que el comando indicado</p> <pre>R2(config)# R2(config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)#</pre>
<p>Mensaje MOTD</p>	<p>Creemos un mensaje de bienvenida en los dispositivos el cual aparece inmediatamente querramos ingresar a un dispositivo en particular.</p> <pre>Banner motd % SOLO SE PERMITE ACCESO A FERNANDO TRUJILLO%</pre>

<p>Interfaz S0/0/0</p>	<p>Establezca la descripción  Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.  Activar la interfaz</p> <pre> Interface serial 0/0/0 Description connection to R1 Ip address 172.16.1.2 255.255.255.252 Ip nat inside Ipv6 address 2001:DB8:ACAD:1::2/64 </pre>
<p>Interfaz S0/0/1</p>	<p>Establecer la descripción  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.  Establecer la frecuencia de reloj en 128000.  Activar la interfaz</p> <pre> Interface serial 0/0/0 Description connection to R3 Ip address 172.16.2.2 255.255.255.252 Ip nat inside Ipv6 address 2001:DB8:ACAD:2::2/64 Clock rate 128000 </pre>

<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Establecer la descripción.  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.  Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.  Activar la interfaz</p> <pre> Interface gb 0/0 Description connection to Internet Ip address 209.165.200.233 255.255.255.248 Ip nat inside Duplex auto Speed auto Ipv6 address 2001:DB8:ACAD:A::1/64 </pre>
<p>Interfaz loopback 0 (servidor web simulado)</p>	<p>Establecer la descripción.  Establezca la dirección IPv4.</p> <pre> R2#config Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z. R2(config)# R2(config)#int g0/1 R2(config-if)#ip address 10.10.10.1 255.255.255.0 R2(config-if)#no shutdown </pre>
<p>Ruta predeterminada</p>	<p>Configure una ruta IPv4 predeterminada de G0/0.  Configure una ruta IPv6 predeterminada de G0/0.</p> <pre> ip classless ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 ! ip flow-export version 9 ! ipv6 route ::/0 GigabitEthernet0/0 </pre>

- Configuración del servidor WEB.

Figura 4 - configuración del servidor WEB.



Fuente: Autoría propia.

## 2.6 Configuración de R3.

Procedemos ya en este punto a realizar la configuración de R3, proceso que se lleva a continuación:

Tabla 4 – configuración R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Desactivamos la búsqueda DNS ahorrando recursos: No ip domain lookup
Nombre del router	Debemos identificar de manera única cada uno de los dispositivos. Hostname R3
Contraseña de exec privilegiado cifrada	Configuramos las diferentes contraseñas con el fin de garantizar la integridad de los mismos. Enable secret class

<p>Contraseña de acceso a la consola</p>	<p>Recordemos que este es un puerto físico, por consiguiente si alguien tiene acceso a los equipos puede estar realizando algún tipo de modificación que perjudique el funcionamiento del mismo.</p> <p>Line console 0 Password cisco Login</p>
<p>Contraseña de acceso Telnet</p>	<p>Creamos las contraseñas de las líneas virtuales VTY que me permitirán el acceso remoto mediante TELNET:</p> <p>Line vty 0 4 Password cisco login</p>
<p>Cifrar las contraseñas de texto no cifrado</p>	<p>Procedemos a encriptar nuestras contraseñas:</p> <p>Service password-encryption</p>
<p>Mensaje MOTD</p>	<p>Creemos un mensaje de bienvenida en los dispositivos el cual aparece inmediatamente querramos ingresar a un dispositivo en particular.</p> <p>Banner motd % SOLO SE PERMITE ACCESO A FERNANDO TRUJILLO%</p>
<p>Interfaz S0/0/1</p>	<p>Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</p> <p>Interface serial0/0/1 Description connection to R2 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::1/64</p>

Interfaz loopback 4	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>Interface loopback4 Ip address 192.168.4.1 255.255.255.0</pre>
Interfaz loopback 5	<p>Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.</p> <pre>Interface loopback5 Ip address 192.168.5.1 255.255.255.0</pre>
Interfaz loopback 6	<p>Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred.</p> <pre>Interface loopback6 Ip address 192.168.6.1 255.255.255.0</pre>
Interfaz loopback 7	<p>Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>Interface loopback7 Ipv6 address 2001:DB8:ACAD:3::1/64</pre>
Rutas predeterminadas	<p>Estas rutas se configuran para no descartar los paquetes cuando nuestro dispositivo no tiene la ruta, es como un último recurso:</p> <pre>Ip route 0.0.0.0 0.0.0.0 serial 0/0/1 Ipv6 route ::/0 serial 0/0/1</pre>

## 2.7 Configuración de S1.

La configuración del S1 incluye las siguientes tareas:

*Tabla 5 – configuración S1.*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	Procedemos a desactivar la búsqueda de DNS:  No ip domain lookup
Nombre del switch	Identificamos nuestros dispositivos:  Hostname S1
Contraseña de exec privilegiado cifrada	Creamos nuestras contraseñas:  Enable secret class
Contraseña de acceso a la consola	Configuramos la contraseña del Puerto de consola:  Line console 0 Password cisco Login
Contraseña de acceso Telnet	ingresamos las contraseñas a las lineas virtuales.  Lne vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Configuramos nuestro mensaje.  Service password-encryption
Mensaje MOTD	Banner motd % SOLO SE PERMITE ACCESO A FERNANDO TRUJILLO%

## 2.8 Configuración de S3

Procedemos en este punto a realizar la configuración de S3, proceso que se indica a continuación:

*Tabla 6 – configuración S3.*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password cisco Login
Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Banner motd % SOLO SE PERMITE ACCESO A FERNANDO TRUJILLO%

## 2.9 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:

Recordemos que en este punto ya tenemos configuradas las interfaces para nuestro caso de los routers R1 y R2, procedemos a dejar plasmadas las direcciones de las interfaces de los mismos:



Tabla 7 – prueba de conectividad.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.2.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

Figura 5 – PING desde R1.

```
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
```

Fuente: Autoría propia

Figura 6 – PING desde R2.

```
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
```

Fuente: Autoría propia

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

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

#### 3.1 Configuración VLAN, routing y seguridad en S1.

La configuración del S1 incluye las siguientes tareas:

Tabla 8 – configuración interfaces S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican  Interface vlan 21
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología  Interface vlan 99 Ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado.  Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa  interface FastEthernet0/3 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range, de esta manera no debemos configurar cada interface de manera individual, aprovechamos y configuramos igual como modo acceso.  int range fastethernet 1-2, fa0/4, fa0/6-24, g1/1-2 switchport mode access

Asignar F0/6 a la VLAN 21	Ya que tenemos creadas las VLAN debemos proceder a indicar que interface es asignada a cada una de ellas.  interface F0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown

### 3.2 Configuración VLAN, routing y seguridad en S3.

Procedemos a configurar ahora el dispositivo S3 incluye las siguientes tareas:

*Tabla 9 – Configuración interfaces S3*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.  Interface fastethernet 0/18 Switchport Access vlan 23 Switchport mode access
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología  Interface vlan 99 Ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.  Ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa  Interface fastethernet0/3 Switchport mode trunk
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range  int range fa 0/1-2, fa0/4-24, g1/1-2 switchport mode access
Asignar F0/18 a la VLAN 23	Luego de creadas las VLAN procedemos asigna las diferentes interfaces a cada una de ellas.  interface F0/18 switchport mode access switchport access vlan 23
Apagar todos los puertos sin usar	interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, G0/1-2 shutdown

### 3.3 Configuración de subinterfaces y encapsulación en R1.

Las tareas de configuración para R1 incluyen las siguientes, recordemos que ya tenemos configuradas las interfaces y las VLAN, ahora debemos proceder a configurar el ROUTER R1 el cual me va a permitir este intercambio mediante la encapsulación:

*Tabla 10 – configuración interfaces R1*

<b>Elemento o tarea de configuración</b>	<b>Especificación</b>
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz</p> <pre>interface GigabitEthernet0/1.21 description Accounting LAN encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0</pre>
Configurar la subinterfaz 802.1Q .23 en G0/1	<p>Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz</p> <pre>interface GigabitEthernet0/1.23 description Accounting LAN encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0</pre>
Configurar la subinterfaz 802.1Q .99 en G0/1	<p>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</p> <pre>interface GigabitEthernet0/1.99 description Accounting LAN encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0</pre>
Activar la interfaz G0/1	<p>Ya que tenemos configuradas las subinterfaces debemos proceder a configurar la interface, como indicamos a continuación:</p> <pre>interface g0/1 no shutdown</pre>

### 3.4 Verificar la conectividad de la red

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

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

Asignamos la dirección IP que se configuro con anterioridad con el fin de proceder a realizar la verificación por medio del comando PING.

*Tabla 11 – prueba de conectividad desde los ROUTERS*

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

*Figura 7 – PING desde S1.*

```
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

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 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

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 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

*Fuente: Autoría propia*

Figura 8 – PING desde S1.

```
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 = 0/4/16 ms
```

```
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 100 percent (5/5), round-trip min/avg/max = 0/2/8 ms

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 100 percent (5/5), round-trip min/avg/max = 0/4/20 ms
```

Fuente: Autoría propia

## 4. Configurar el protocolo de routing dinámico OSPF

### 4.1 Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12 – configuración de OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 0 router-id 1.1.1.1

<p>Anunciar las redes conectadas directamente</p>	<p>Recordemos, que en este punto debemos anunciar cada una de las redes que esta conectada al dispositivo de manera individual con respectiva wildcard.</p> <pre>network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0</pre>
<p>Establecer todas las interfaces LAN como pasivas</p>	<p>Configuramos las interfaces LAN como passive con el fin de que el Router no envíe sus mensajes de propagación por estos.</p> <pre>passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99</pre>
<p>Desactive la sumarización automática</p>	<p>Debemos desactivar la sumarización con el fin de que las rutas se propaguen de manera individual.</p> <pre>no auto-summary</pre>





Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 router-id 2.2.2.2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. network 172.16.2.0 0.0.0.3 area 0 network 172.16.1.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	Recordemos que este proceso lo hacemos con el fin de que el Router no envíe los mensajes de propagación por estas, lo cual no sería necesario. passive-interface lo0 passive-interface g0/1
Desactive la sumarización automática.	no auto-summary

Figura 10 - Configurar OSPF en el R2

```

R2
Physical  Config  CLI  Attributes
IOS Command Line Interface
ip nat inside
ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Serial10/0/1
description Connection to R3
ip address 172.16.2.2 255.255.255.252
ip nat inside
ipv6 address 2001:DB8:ACAD:2::2/64
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
passive-interface Loopback0
network 172.16.2.0 0.0.0.3 area 0
network 172.16.1.0 0.0.0.3 area 0
!
ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.237
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0
!
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
in access-list standard 192.168.4.0

```

Fuente: Autoría propia

### 4.3 Configurar OSPFv3 en el R3.

La configuración del R3 incluye las siguientes tareas:

Tabla 14 – configuración de OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	Anunciamos cada una de las redes que esta conectada al dispositivo:  network 172.16.2.0 0.0.0.3 area 0 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
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	De esta manera evitamos la propagación de mensaje por estas interfaces:  passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	no auto-summary

Figura 11 - Configurar OSPFv3 en el R3

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.0.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
```

Fuente: Autoría propia.

#### 4.4 Verificar la información de OSPF.

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

Tabla 15 – comandos de verificación 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
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show ip ospf neighbor

Figura 12 – show ip protocols.

```
R1#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 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:10:54
    2.2.2.2          110          00:05:43
    3.3.3.3          110          00:05:43
  Distance: (default is 110)
```

Fuente: Autoría propia.

Figura 13 - show ip route OSPF.

```

R1#show ip route OSPF
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.16.2.0 [110/128] via 172.16.1.2, 00:12:08, Serial0/0/0
    192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/129] via 172.16.1.2, 00:06:45, Serial0/0/0
    192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/129] via 172.16.1.2, 00:06:45, Serial0/0/0
    192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/129] via 172.16.1.2, 00:06:45, Serial0/0/0
R1#

```

Fuente: Autoría propia

Figura 14 - show ip OSPF neighbor

```

R1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
2.2.2.2          0    FULL/ -         00:00:33   172.16.1.2   Serial0/0/0
R1#

```

Fuente: Autoría propia

## 5. Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 – configuración de DHCP.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Debemos indicar el rango de direcciones que en este caso vamos a excluir:  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	Debemos indicar el rango de direcciones que en este caso vamos a excluir:  ip dhcp excluded-address 192.168.23.1 192.168.23.20

<p>Crear un pool de DHCP para la VLAN 21.</p>	<p>Creamos el POOL de direcciones que vamos a utilizar para DHCP para la VLAN 21, siguiente las indicaciones dadas:</p> <p>Nombre: ACCT  Servidor DNS: 10.10.10.10  Nombre de dominio: ccna-sa.com  Establecer el gateway predeterminado</p> <pre>ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10 domain-name ccna-sa.com</pre>
<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Creamos el POOL de direcciones que vamos a utilizar para DHCP para la VLAN 23, siguiente las indicaciones dadas:</p> <p>Nombre: ENGNR  Servidor DNS: 10.10.10.10  Nombre de dominio: ccna-sa.com  Establecer el gateway predeterminado</p> <pre>ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 domain-name ccna-sa.com</pre>

Figura 15 - Implementar DHCP y NAT para IPv4

```
hostname R1
!
!
enable secret 5 $!$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ACCT
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
dns-server 10.10.10.10
ip dhcp pool ENGR
network 192.168.23.0 255.255.255.0
default-router 192.168.23.1
dns-server 10.10.10.10
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
license udi pid CISCO1941/K9 sn FTX15247J4S
!
!
!
```

Fuente: Autoría propia

## 5.2 Configurar la NAT estática y dinámica en el R2

La configuración del **R2** incluye las siguientes tareas:

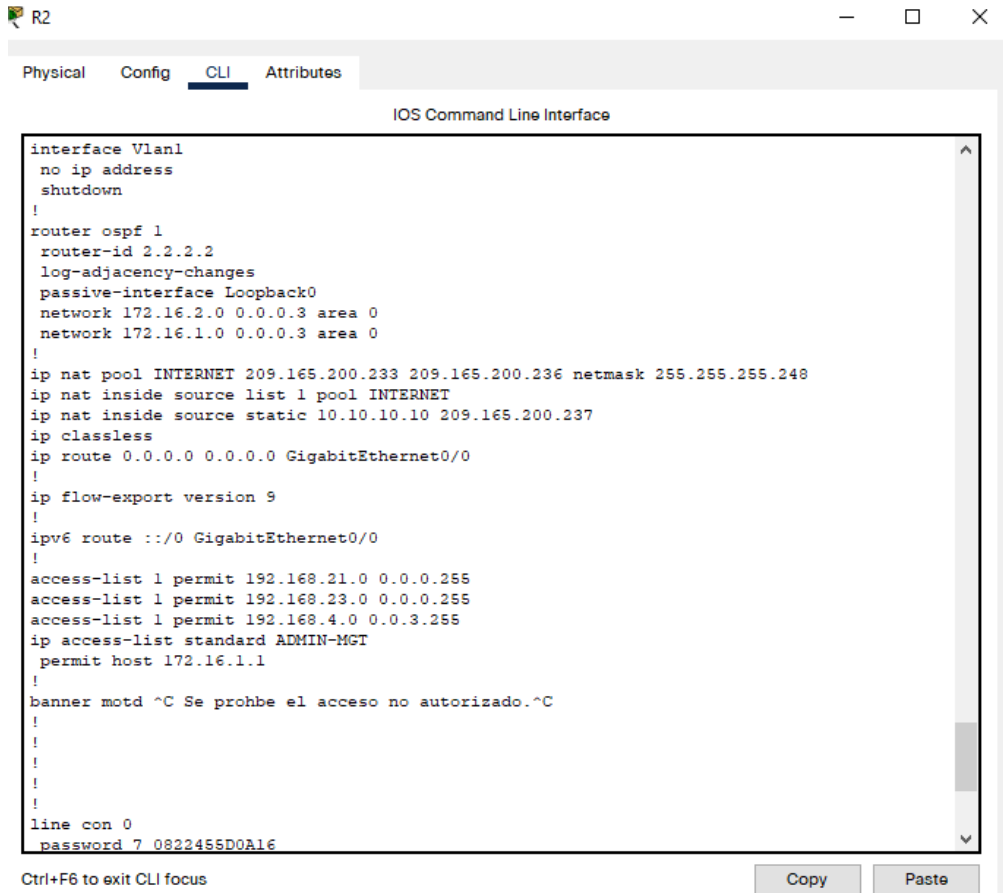
Tabla 17 – configuración NAT estático Y dinámico.

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Vamos a crear la cuenta siguiendo estas especificaciones:</p> <p>Nombre de usuario: <b>webuser</b>            Contraseña: <b>cisco12345</b>            Nivel de privilegio: <b>15</b></p> <p>User webuser privilege 15 secret cisco 12345</p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>ip http server</p> <p>comando no es soportado por Packet Tracer</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>ip http authentication local</p> <p>packet tracer no soporta este comando</p>
<p>Crear una NAT estática al servidor web.</p>	<p>Dirección global interna: <b>209.165.200.229</b></p> <p>Ip nat inside source static 10.10.10.10 209.165.200.229</p>
<p>Asignar la interfaz interna y externa para la NAT estática</p>	<p>Debemos observar el dispositivo en el cual estamos configurando, esto con el fin de tener claridad cual es la interface de salida y la de entrada.</p> <p>interface g0/0            ip nat outside            interface g0/1            ip nat inside</p>



<p>Configurar la NAT dinámica dentro de una ACL privada</p>	<p>Lista de acceso: 1</p> <p>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1</p> <p>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3</p> <p>Debemos tener en claro las indicaciones anteriores para crear estas ACL:</p> <pre>Access-list 1 permit 192.168.21.0 0.0.0.255 Access-list 1 permit 192.168.23.0 0.0.0.255 Access-list 1 permit 192.168.4.0 0.0.3.255</pre>
<p>Defina el pool de direcciones IP públicas utilizables.</p>	<p>Nombre del conjunto: <b>INTERNET</b></p> <p>El conjunto de direcciones incluye: <b>209.165.200.225 – 209.165.200.228</b></p> <pre>ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248</pre>
<p>Definir la traducción de NAT dinámica</p>	<p>Hacemos el NAT dinámico con el fin de poder hacer la traducción empleando la lista 1.</p> <pre>ip nat inside source list 1 pool INTERNET</pre>

Figura 16 - Configurar la NAT estática y dinámica en el R2



```
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
passive-interface Loopback0
network 172.16.2.0 0.0.0.3 area 0
network 172.16.1.0 0.0.0.3 area 0
!
ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.237
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0
!
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
ip access-list standard ADMIN-MGT
permit host 172.16.1.1
!
banner motd ^C Se prohbe el acceso no autorizado.^C
!
!
!
!
!
line con 0
password 7 0822455D0A16
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente: Autoría propia

### 5.3 Verificar el protocolo DHCP y la NAT estática

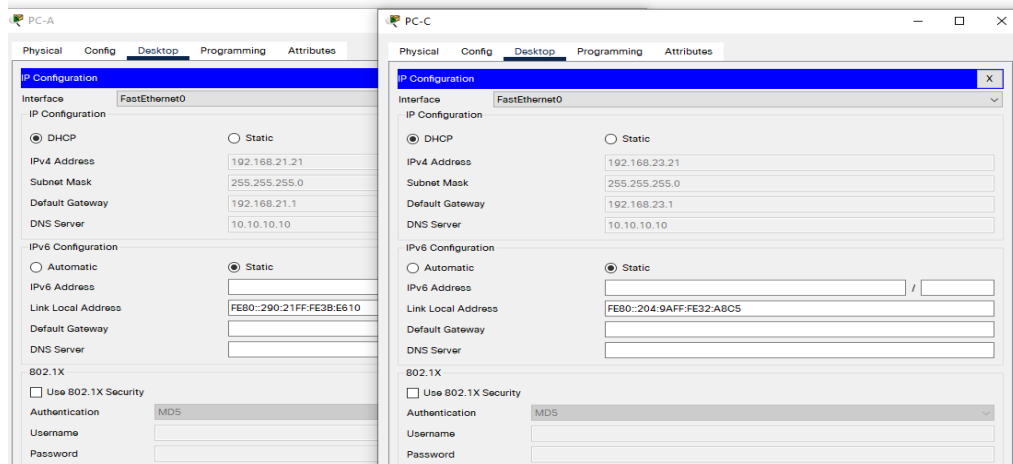
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 18 – verificación de DHCP y NAT.

<b>Prueba</b>	<b>Resultados</b>
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<pre>C:\&gt;ipconfig /all  FastEthernet0 Connection:(default port)  Connection-specific DNS Suffix.: Physical Address .....0090.213B.E610 Link-local IPv6 Address .....: FE80::290:21FF:FE3B:E610 IP Address .....: 192.168.21.21 Subnet Mask .....: 255.255.255.0 Default Gateway .....: 192.168.21.1 DNS Servers .....: 10.10.10.10 DHCP Servers .....: 192.168.21.1 DHCPv6 Client DUID.....: 00-01-00-01-A2-07 32-C5-00-90-21-3B-E6-10</pre>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<pre>C:\&gt;ipconfig /all  FastEthernet0 Connection:(default port)  Connection-specific DNS Suffix.: Physical Address .....0004.9A32.A8C5 Link-local IPv6 Address .....: FE80::204:9AFF:FE32:A8C5 IP Address .....: 192.168.23.21 Subnet Mask .....: 255.255.255.0 Default Gateway .....: 192.168.23.1 DNS Servers .....: 10.10.10.10 DHCP Servers .....: 192.168.23.1 DHCPv6 Client DUID.....: 00-01-00-01-CE-16-91-9B-00-04-9A-32-A8-C5</pre>

<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p><b>Nota:</b> Quizá sea necesario deshabilitar el firewall de la PC.</p>	<pre>C:\&gt;ping 192.168.23.21</pre> <p>Pinging 192.168.23.21 with 32 bytes of data:</p> <p>Request timed out.  Reply from 192.168.23.21: bytes=32 time=1ms TTL=127  Reply from 192.168.23.21: bytes=32 time&lt;1ms TTL=127  Reply from 192.168.23.21: bytes=32 time&lt;1ms TTL=127</p> <p>Ping statistics for 192.168.23.21:  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  Approximate round trip times in milli-seconds:  Minimum = 0ms, Maximum = 1ms, Average = 0ms</p>
<p>Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237)  Iniciar sesión con el nombre de usuario <b>webuser</b> y la contraseña <b>cisco12345</b></p>	<p>Exitoso.</p>

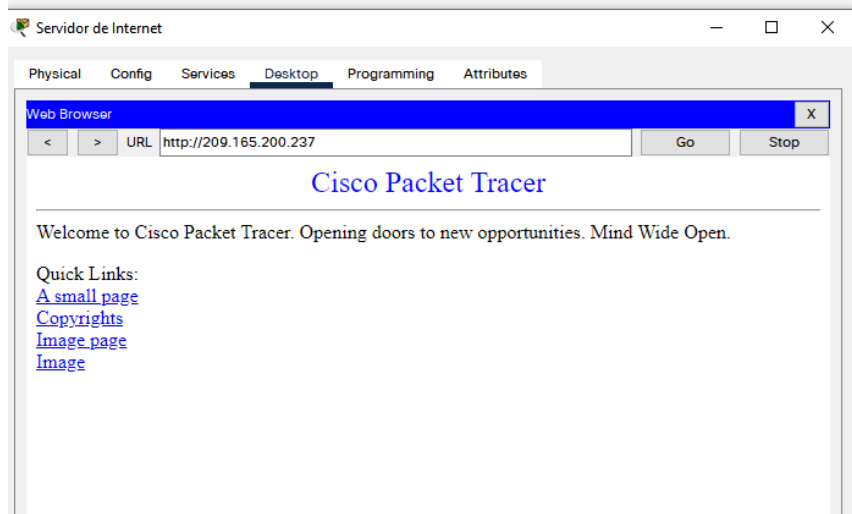
Figura 17 - verificación de DHCP.



Fuente: Autoría propia.

- Acceso al servidor web desde el PC Internet

*Figura 18 - verificación servicio WEB.*



*Fuente: Autoría propia.*

## 6. Configurar NTP

*Tabla 19 – NTP*

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	<b>5 de marzo de 2016, 9 a. m.</b>
Configure R2 como un maestro NTP.	Nivel de estrato: <b>5</b>
Configurar R1 como un cliente NTP.	Servidor: <b>R2</b>
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar

<p>Verifique la configuración de NTP en R1.</p>	<pre>R1#show ntp associations  address      ref clock    st  when  poll reach delay  offset      disp *~172.16.1.2 127.127.1.1 5   2     64   1 4.00        1.00        0.00 * sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured</pre>
---	--

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

### 7.1 Restringir el acceso a las líneas VTY en el R2

Tabla 20 – Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: <b>ADMIN-MGT</b>  Ip Access-list standard ADMIN-MGT Permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!  User Access Verification  Password: R2>en Password: R2#

- TELNET desde R1 a R2

Figura 19 - TELNET desde R1 a R2

```

R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open Se prohbe el acceso no autorizado.

User Access Verification

Password:
R2>enable
Password:
R2#
R2#
R2#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  209.165.200.233 YES manual up          up
GigabitEthernet0/1  10.10.10.1      YES manual up          up
Serial0/0/0        172.16.1.2      YES manual up          up
Serial0/0/1        172.16.2.2      YES manual up          up
Vlan1             unassigned      YES unset  administratively down down
R2#

```

Fuente: Autoría propia.

## 7.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 21 – comando SHOW.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	<pre> show access-lists  R2# R2#show access-lists Standard IP access list 1  10 permit 192.168.21.0 0.0.0.255 (6 match(es))  20 permit 192.168.23.0 0.0.0.255 (2 match(es))  30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT  10 permit host 172.16.1.1 (2 match(es))  R2# </pre>
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p><b>Nota:</b> Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.</p> <p>Show ip nat translation Show ip nat statics</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>clear ip nat translations *</p>

- Verificamos las traducciones NAT en R2.

Figura 20 - verificación de NAT.

```

R2#show ip nat translations
Pro  Inside global      Inside local        Outside local      Outside global
icmp 209.165.200.233:13 192.168.23.21:13 209.165.200.238:13 209.165.200.238:13
icmp 209.165.200.233:14 192.168.23.21:14 209.165.200.238:14 209.165.200.238:14
icmp 209.165.200.233:15 192.168.23.21:15 209.165.200.238:15 209.165.200.238:15
icmp 209.165.200.233:16 192.168.23.21:16 209.165.200.238:16 209.165.200.238:16
icmp 209.165.200.233:17 192.168.23.21:17 209.165.200.238:17 209.165.200.238:17
icmp 209.165.200.233:18 192.168.23.21:18 209.165.200.238:18 209.165.200.238:18
icmp 209.165.200.233:19 192.168.23.21:19 209.165.200.238:19 209.165.200.238:19
icmp 209.165.200.233:20 192.168.23.21:20 209.165.200.238:20 209.165.200.238:20
icmp 209.165.200.234:1 192.168.23.21:1 209.165.200.238:1 209.165.200.238:1
icmp 209.165.200.234:2 192.168.23.21:2 209.165.200.238:2 209.165.200.238:2
icmp 209.165.200.234:3 192.168.23.21:3 209.165.200.238:3 209.165.200.238:3
icmp 209.165.200.234:4 192.168.23.21:4 209.165.200.238:4 209.165.200.238:4
icmp 209.165.200.234:5 192.168.23.21:5 209.165.200.238:5 209.165.200.238:5
icmp 209.165.200.234:6 192.168.23.21:6 209.165.200.238:6 209.165.200.238:6
icmp 209.165.200.234:7 192.168.23.21:7 209.165.200.238:7 209.165.200.238:7
icmp 209.165.200.234:8 192.168.23.21:8 209.165.200.238:8 209.165.200.238:8
--- 209.165.200.237 10.10.10.10 ---
tcp 209.165.200.233:1025 192.168.23.21:1025 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1026 192.168.23.21:1026 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1027 192.168.23.21:1027 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.234:1025 192.168.23.21:1025 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1025 209.165.200.238:1025
tcp 209.165.200.237:80 10.10.10.10:80 209.165.200.238:1026 209.165.200.238:1026

```

Fuente: Autoría propia.



## CONCLUSIONES

- Luego de realizar el proceso de configuración hemos podido verificar que tenemos total conectividad dentro de nuestras redes configuradas, comprendemos el proceso de desarrollo e implementación de nuestra red aplicando para ello comandos específicos para cada una de las situaciones.
- El material de apoyo con el cual se cuenta para el desarrollo del Diplomado es muy completo, y junto con el acompañamiento de los TUTORES fue posible culminar el desarrollo del mismo.
- PACKET TRACER se convirtió en nuestra mano derecha, gracias a este podemos realizar el montaje de la red simulada con el fin de poder verificar el correcto funcionamiento de la misma.
- Veo con agrado que los temas han sido asimilados por nuestra parte, estamos en condiciones de configurar redes de mediana complejidad.
- A todo el direccionamiento IP de la red aplicamos VLSM lo cual nos permitió optimizar el número de direcciones por cada subred de acuerdo a los requerimientos específicos.

## BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. <https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx>

*Cisco Systems Inc. Módulo de estudio CCNA Exploration 4.0. Conceptos y protocolos de enrutamiento. [Documento PDF en línea]. Disponible en: [http://www.mediafire.com/view/5y052miul2vezhj/MODULO\\_DE\\_ESTUDIO\\_CCNA\\_2\\_EXPLORATION.pdf](http://www.mediafire.com/view/5y052miul2vezhj/MODULO_DE_ESTUDIO_CCNA_2_EXPLORATION.pdf) [2014, 19 de Junio]*

CP CCNA 1 I-2014. CCNA Exploration: Aspectos Basicos de Networking [En Linea] Disponible en: <https://1314297.netacad.com/courses/125408> [2014, 4 de Febrero].

CISCO SYSTEM. Modulo Curso de entrenamiento CCNA 1 EXPLORATION (Network Fundamentals y Routing Protocols and Concepts).

## ANEXOS

Anexo 1 Link Descarga Escenario 1

[ESCENARIO 1.pkt](#)

Anexo 2 Link Descarga Escenario 2

[ESCENARIO 2.pkt](#)

Anexo 3 Link Articulo Científico

Anexo 4 Link Video de Sustentación.

<https://vimeo.com/728494758>