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

HENRY GIOVANNI HERNANDEZ BERNAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-PASTO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE TELECOMUNICACIONES
NOVIEMBRE DEL 2021.

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

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR POR EL TITULO DE INGENIERO DE TELECOMUNICACIONES.

HENRY GIOVANNI HERNANDEZ BERNAL

TUTOR
JAVIER RICARDO VASQUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
NOVIEMBRE DEL 2021.

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____
FIRMA

_____
FIRMA

_____
FIRMA

Mi camino a lo largo de mi vida como estudiante ha sido de vital importancia pues gracias a ella he logrado aprender aspectos supremamente importantes para el desarrollo ahora de mi vida profesional. Por esto agradezco tanto a mis profesores como a mi Universidad por haber hecho posible este sueño, por haber hecho posible lograr alcanzar esta nueva meta. Agradezco infinitamente a mi familia pues hace parte fundamental de mi vida y de este proceso, ellos son artífices de todo el proceso llevado para llegar al punto donde estoy.

HENRY GIOVANNI HERNANDEZ BERNAL.

TABLA DE CONTENIDO

Tabla de Figuras

Lista deTablas

GLOSARIO

En esta parte se relacionan todos los conceptos dejando claro la teoría que se siguió como modelo de la realidad de los estudios de caso de redes que son el tema de investigación en este trabajo.

ATM Asyncronous Transmision Mode. Modo de Transmisión Asíncrona. Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2 Gbps. Implementación normalizada (por ITU) de Cell Relay, técnica de conmutación de paquetes que utiliza celdas de longitud fija.

INTERNET. Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

ADSL Asymmetric Digital Subscriber Line. Línea Digital Asimétrica de Abonado. Sistema asimétrico de trasmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades de 1,5 y 6 Megabits por segundo en un sentido y entre 16 y 576 Kilobits en el otro.

BIT Binary Digit. Digito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

ANSI American National Standard Institute. Instituto Nacional Americano de Estándar.

Bandwith Ancho de Banda. Capacidad máxima de un medio de transmisión y/o enlace.

Browser. Navegador. Término aplicado normalmente a los programas que permiten acceder al servicio WWW.

Bridge. Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

DATAGRAM Datagráma. Usualmente se refiere a la estructura interna de un paquete de datos.

INTRANET Se llaman asi a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de internet. Tambien se refiere a las direcciones de red Internet.

Gateway. Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

Byte 1 Byte es un carácter y equivale a 8 bits, 1Kbyte equivale a 1024 bytes.

CSMA/CD Carrier Sense Multiple Access / Collition Detection. Detección de portadora de acceso múltiple / colisión. En este protocolo las estaciones escuchan al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo (time-out) aleatorio.

Cable coaxial: utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado positivo o vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.

DNS Domain Name System. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Ethernet. Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

FTP. File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los potocolos de tranferencia de ficheros mas usado en Internet.

Full Duplex. Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente.

ICMP Internet Control Message Protocol. Protocolo Internet de Control de Mensajes.

ISO International Standard Organization. Organización Internacional de Estándares.

Direcciones IP: es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP sePuede cambiar.

Cable de fibra óptica: un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales

plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Fastethernet: es el nombre de una serie de estándares de IEEE de redes

Host: Un **host o anfitrión** es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web.

LAN: Una **red de área local**, **red local** o **LAN** (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.

Loopback: es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1 y :: 1 para el caso de IPv6.

Mascara de subred: La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP.

OSPF: (Open Shortest Path First) frecuentemente abreviado **OSPF** es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa *cost* como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database*, LSDB) idéntica en todos los enrutadores de la zona.

Packet tracer es la herramienta de aprendizaje y simulación de redes interactiva paralosinstructores y alumnos de CiscoCCNA.Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetesysimular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

RIP: son lassiglas de Routing Information Protocol (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers, (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

Protocolos: es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre

dos puntos finales.

Switch: es un dispositivo de red que funciona como un repartidor y sirve para segmentar una red en diferentes dominios de difusión.

Router: dispositivo intermediario en las redes que se asegura de que la información no va a donde no es necesario; la labor principal de un Router es disipar y coordinar la información perteneciente a las direcciones lógicas de Red en un sistema.

VLSM: Las máscaras de subred de tamaño variable (variable length subnet mask, (VLSM) representan otra delastantas soluciones que se implementaron para el agotamiento de direcciones ip (1987) y otras como la división en subredes (1985), el enrutamiento de interdominio CIDR (1993), NAT y las direcciones ipprivadas.

RESUMEN

Gracias al desarrollo de esta actividad fue fundamental para poder aplicar nuestros conocimientos y desarrollar destrezas en el desarrollo de proyectos de este tipo, y que mejor manera que a través de la solución de estos 2 ESCENARIOS. Profundizaremos mucho más en el tema que tiene que ver con los diferentes medios de transmisión y los dispositivos intermedios que hacen parte de las redes y hacen posible la comunicación. Aplicare todo el conocimiento adquirido en lo que tiene que ver con el direccionamiento IP aplicando VLSM tanto para el direccionamiento IPV4 como también IPV6 y todo el tema relacionado con PROTOCOLOS DE ENRUTAMIENTO haciendo énfasis en los siguientes conceptos: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

Por nuestra modalidad de educación a distancia es de se hace fundamental la utilización del simulador de REDES PACKET TRACER la cual ha sido la posibilidad perfecta para las personas que no disponemos de esos dispositivos físicos podamos aplicar nuestros conocimiento y destrezas adquiridas.

ABSTRACT

Thanks to the development of this activity, it was essential to be able to apply our knowledge and develop skills in the development of projects of this type, and what better way than through the solution of these 2 SCENARIOS. We will delve much more into the subject that has to do with the different transmission media and the intermediate devices that are part of the networks and make communication possible. I will apply all the knowledge acquired in what has to do with IP addressing applying VLSM for both IPV4 and IPV6 addressing and all the subject related to ROUTING PROTOCOLS emphazing the following concepts: CISCO, CCNA, Switching, Routing, Networks, Electronics.

Due to our distance education modality, the use of the REDES PACKET TRACER simulator is essential, which has been the perfect possibility for people who do not have these physical devices to apply our knowledge and acquired skills.

INTRODUCCION

La tecnología, las telecomunicaciones se han vuelto parte fundamental dentro de nuestras vidas, las mismas ya están inmersas en todos los campos de nuestras vidas, ya no importa el ámbito o el tipo de los mismos todos deben formar parte o desarrollarse de menra conjunta con la tecnología, ya nada se puede desconectar, muchas cosas deben funcionar 24X7 y de esta manera poder suplir las necesidades de un universo que cambia constantemente.

La presente actividad se van a desarrollar 2 ESCENARIOS los cuales se ajustan muy bien a actividades que muy posiblemente encontremos en nuestro ambiente laboral, cada uno de estos escenarios cuentan con una cantidad de exigencias las cuales debemos suplir mediante el diseño y contaje de la red indicada, gracias a todos estos procesos lo que vamos a lograr es que afiancemos todo lo adquirido a lo largo de nuestra carrera.

La parte de la implementación como tal se hará empleando el simulador de PACKET TRACER elemento fundamental en el presente diplomado gracias al cual podemos aplicar cada uno de los elementos adquiridos. Dentro de los escenarios vamos a poner en práctica todo lo relacionado a protocolo OSPF, VLANS, VLSM DHCP.

1. JUSTIFICACION

Como ingenieros, independiente de nuestra rama de trabajo es fundamental el manejo a la perfección de todo lo relacionado con conceptos, configuración de equipos que hacen parte de una RED COMPUTACIONAL.

Debemos formarnos integralmente y prepararnos para afrontar un mercado muy exigente y en lo posible estar en la parte superior gracias a nuestra preparación y nuestras habilidades desarrolladas.

CISCO es una de las organizaciones más importantes dentro de la rama de las TECNOLOGÍAS, no solo por sus dispositivos sino también como academia. Es por esto y gracias a los convenios con la Universidad que debemos aprovechar al máximo este proceso de formación y aplicarlo dentro de nuestra vida profesional.

2. OBJETIVOS

2.1 Objetivo general

Solución de los 2 escenarios empleando tecnología CISCO mediante la utilización del simulador de PACKT TRACER.

2.2 Objetivos Específico

- Profundizar mucho más en el manejo de la herramienta de PACKET TRACER como elemento fundamental para ampliar y afianzar mi conocimiento.
- Mostrar que con esfuerzo y dedicación podemos lograr las metas profesionales que deseemos.
- Comprender la importancia de trabajar en grupo como una herramienta poderosa a la hora de lograr los objetivos planteados.
- Configurar los dispositivos finales e intermediarios en las redes.
- Conocer los diferentes protocolos de enrutamiento y envío de paquetes entre redes, teniendo en cuenta el uso y administración adecuado del Sistema Operativo de Internet working (IOS).

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

Topología

Figura 1: Topología escenario 1

Fuente: Autor.

Figura 1: Topología escenario 1

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

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 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.

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.**36**.0 donde X corresponde a los últimos dos dígitos de su cédula.

RED	N° IP	dir red	masc	/		1re IP	ultima IP	broadcast	N° HOST
LAN 1	100	192.168.36.0	255.255.255.128	25		192.168.36.1	192.168.36.126	192.168.36.127	126
LAN 2	50	192.168.36.128	255.255.255.192	26		192.168.36.129	192.168.36.190	192.168.36.191	62

Tabla 1: Subneteo red.

Item	Requerimiento
Dirección de Red	192.168.**36**.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 192.168.36.1 / 255.255.255.128
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.36.129 / 255.255.255.192
S1 SVI	Segunda dirección de host de la subred

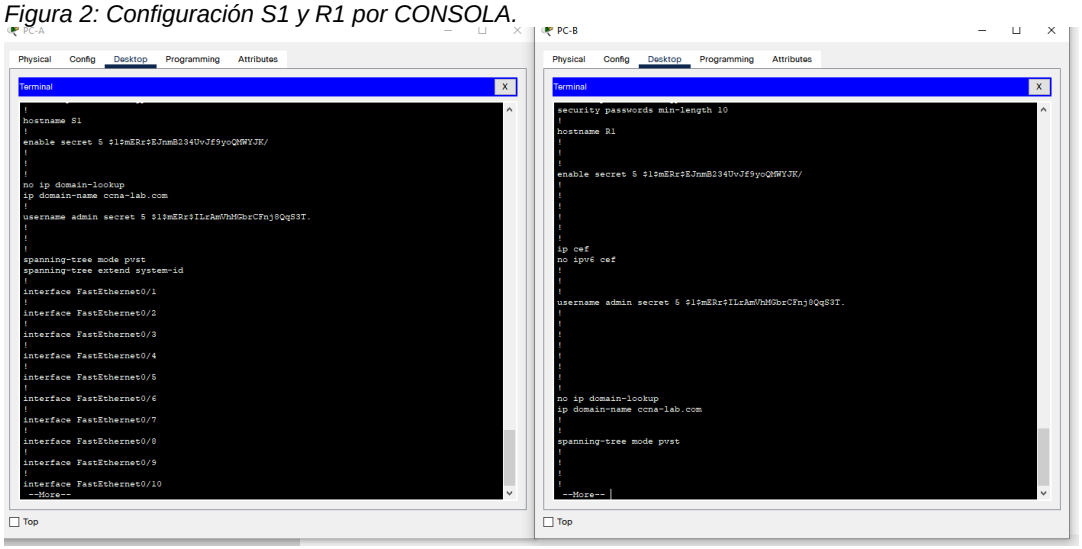
	LAN1 192.168.36.2 / 255.255.255.128
PC-A	Última dirección de host de la subred LAN1 192.168.36.126 / 255.255.255.128
PC-B	Última dirección de host de la subred LAN2 192.168.36.190 / 255.255.255.192

Tabla 2: asignación direcciones interfaces.

Parte 3: Configure aspectos básicos

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

Figura 2: Configuración S1 y R1 por CONSOLA.



Fuente: Autor.

Parte 4: configurar los ajustes básicos

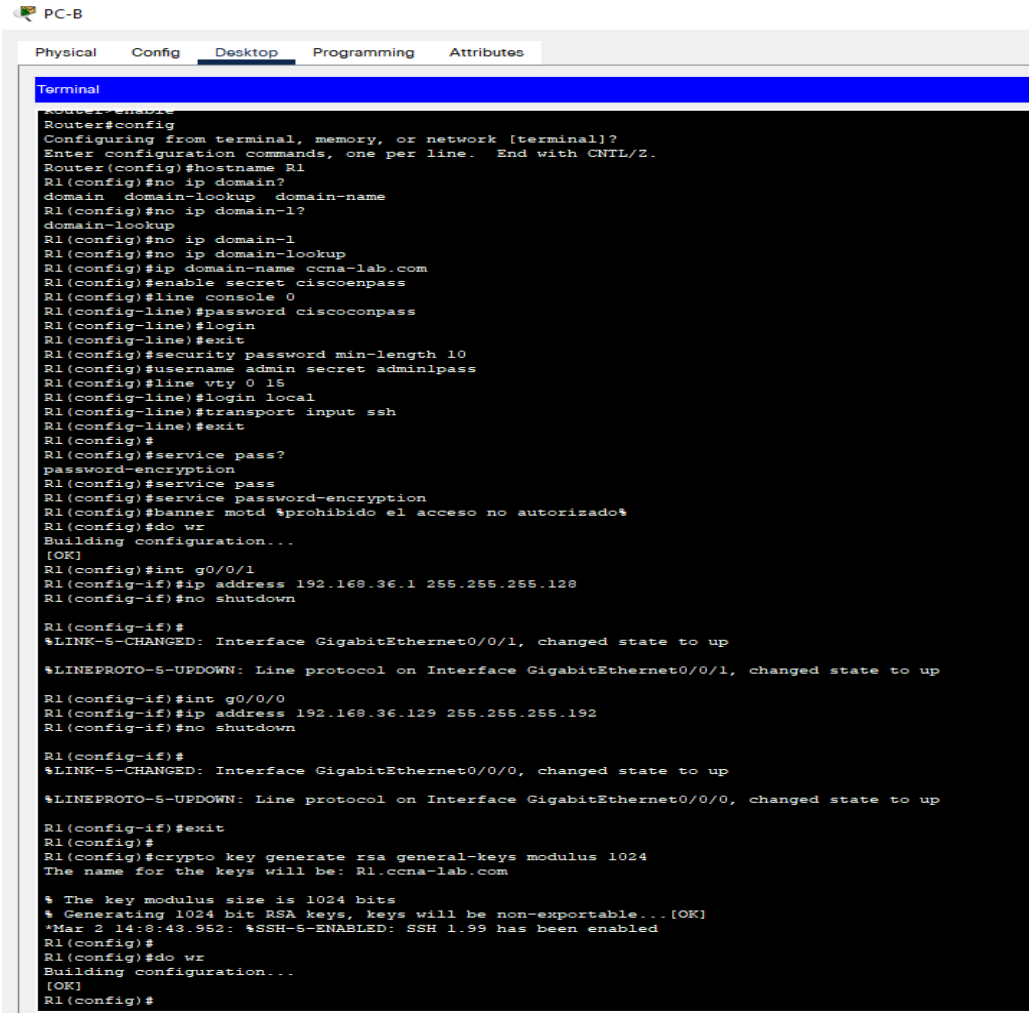
Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del router	hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass line console 0 password ciscoconnpass login
Establecer la longitud mínima para las contraseñas	10 caracteres security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local
Configurar VTY solo aceptando SSH	transport input ssh login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Configure un MOTD Banner	banner motd % Se prohíbe el acceso no autorizado.%

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 crypto key generate rsa general-keys modulus 1024

Tabla 3: configuración básica router 1.

Figura 3: Configuración Router R1 por CONSOLA.



Fuente: Autor.

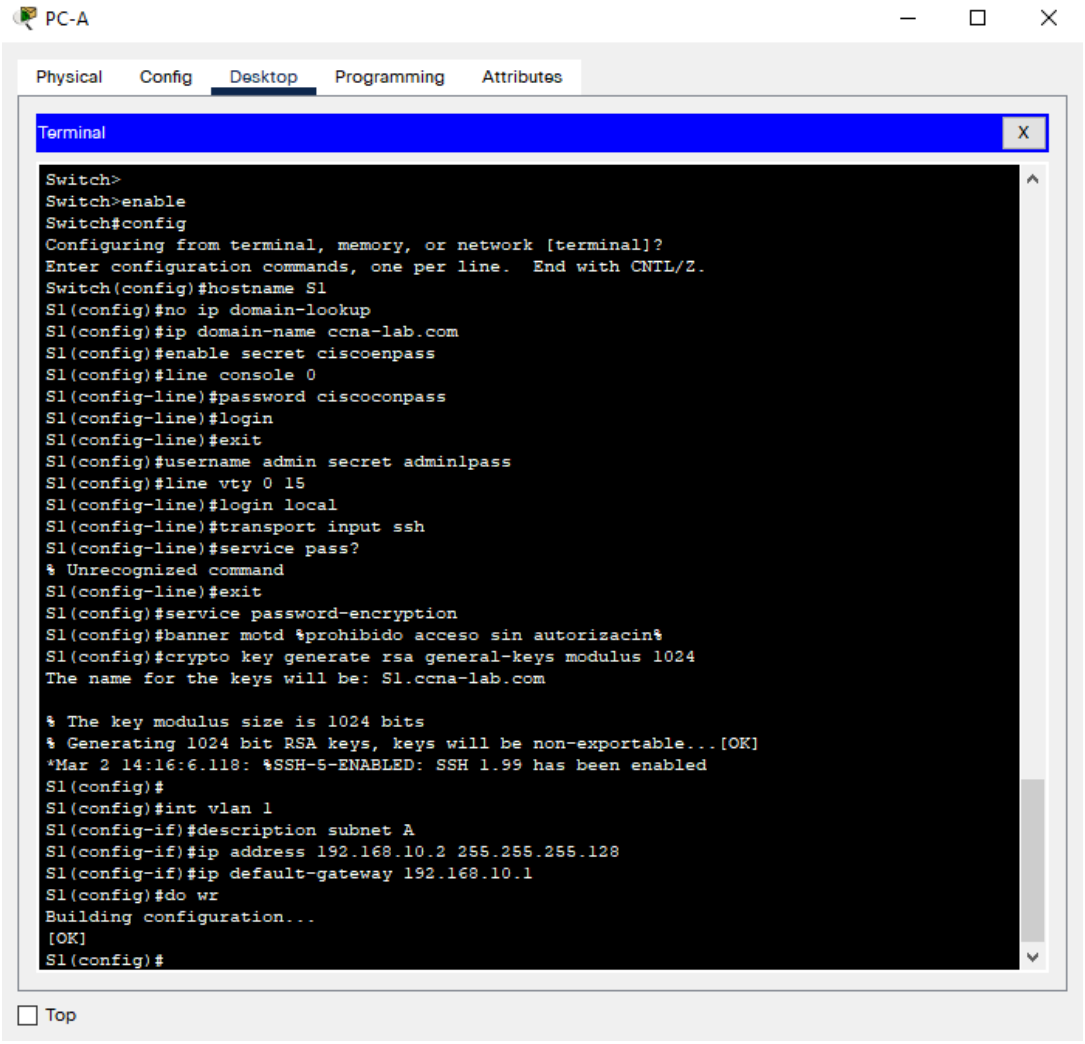
Las tareas de configuración de **S1** incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1** hostname S1
Nombre de dominio	**ccna-lab.com** ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** line console 0 password ciscoconpass login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encyption

Configurar un MOTD Banner	banner motd % Se prohíbe el acceso no autorizado.%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** 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 192.168.36.2 255.255.255.128
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla dedireccionamiento. ip default-gateway 192.168.36.1

Tabla 4: configuración básica S1.

Figura 4: Configuración S1 por CONSOLA.



Fuente: Autor.

Paso 2. Configurar los equipos

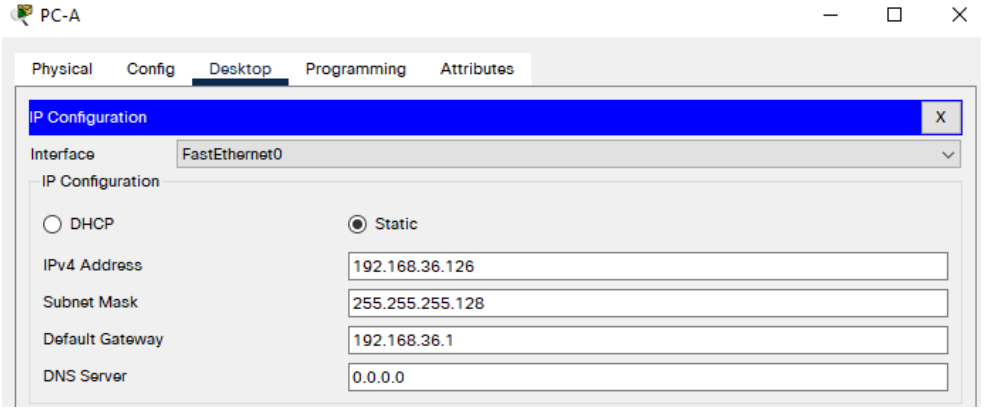
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre lasconfiguraciones de red del host con el comando **ipconfig /all**.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	
Dirección IP	192.168.36.126

Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.36.1

Tabla 5: configuración PC-A.

Figura 5: Configuración IP PC – A.

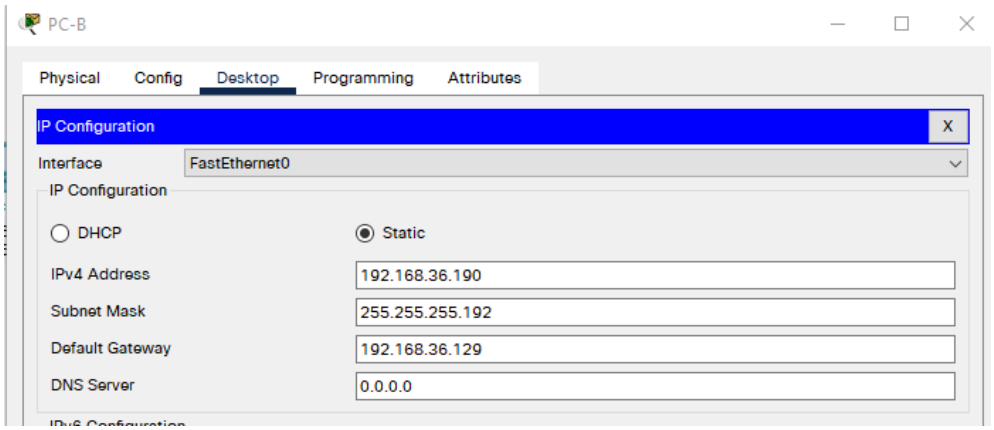


Fuente: Autor.

PC-B Network Configuration	
Descripción	PC-B
Dirección física	
Dirección IP	192.168.36.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.36.129

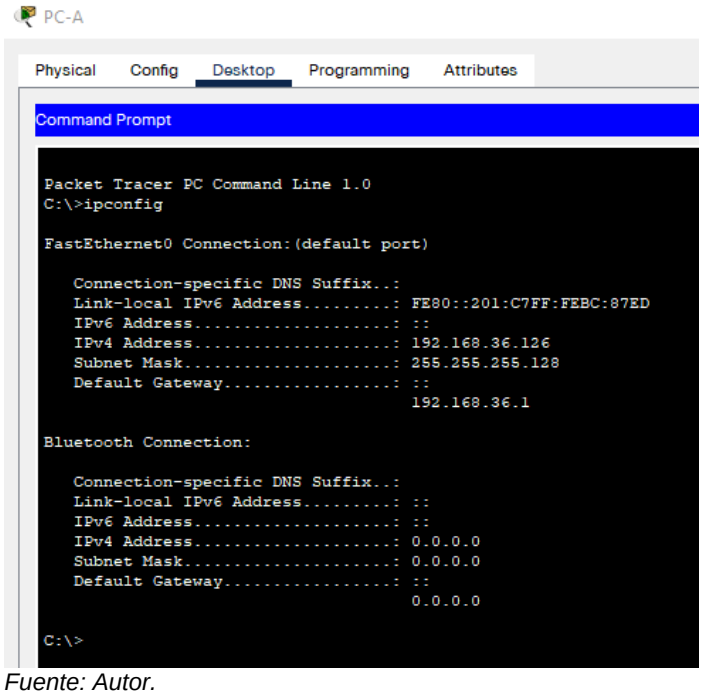
Tabla 6: configuración PC-B.

Figura 6: Configuración IP de la PC-B.



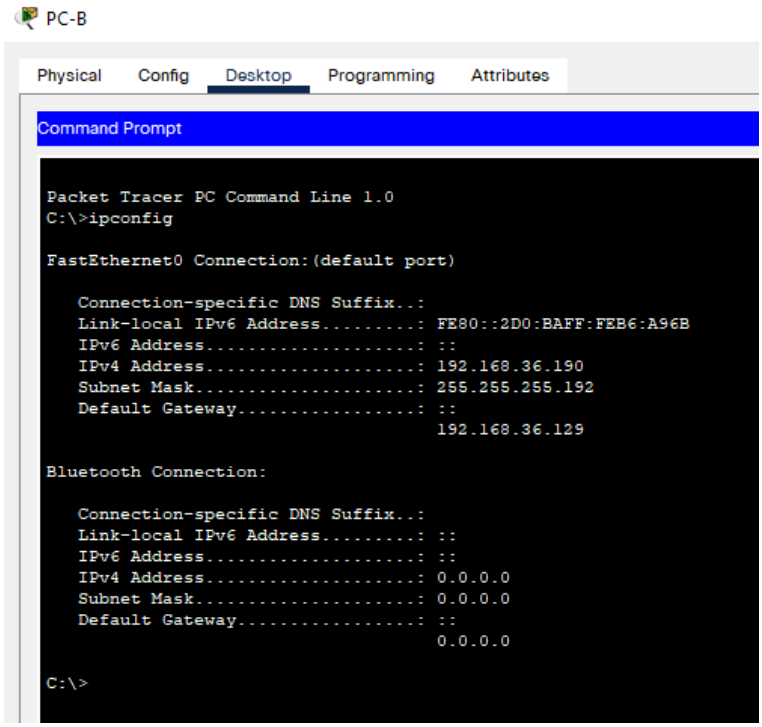
Fuente: Autor.

Figura 7: verificación IP – PC-A.



Fuente: Autor.

Figura 8: verificación IP – PC-B.

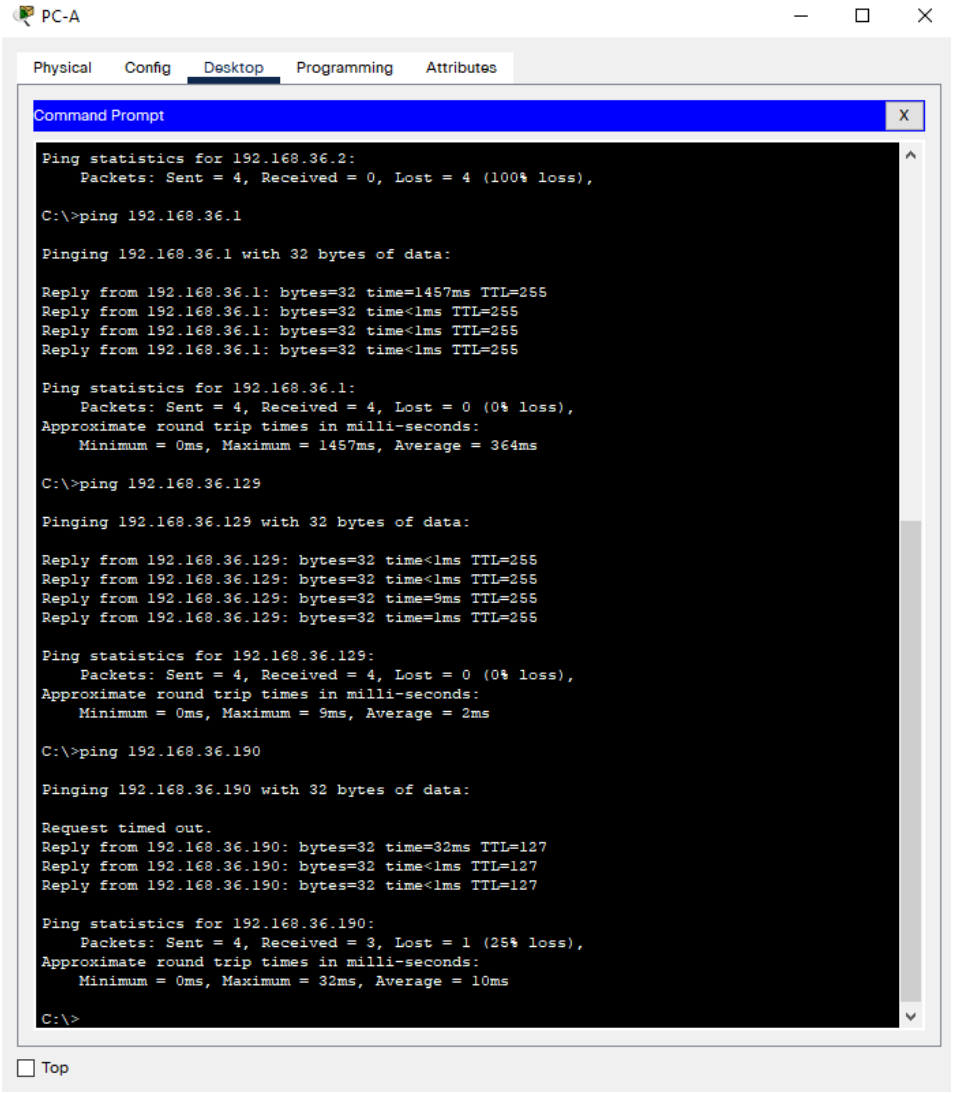


Fuente; Autor.

Procedemos a realizar las respectivas proveas de conectividad:

- Desde PCA hacia los diferentes puertos de la red.

Figura 9: PING desde PC- A hacia los diferentes puntos de la RED.

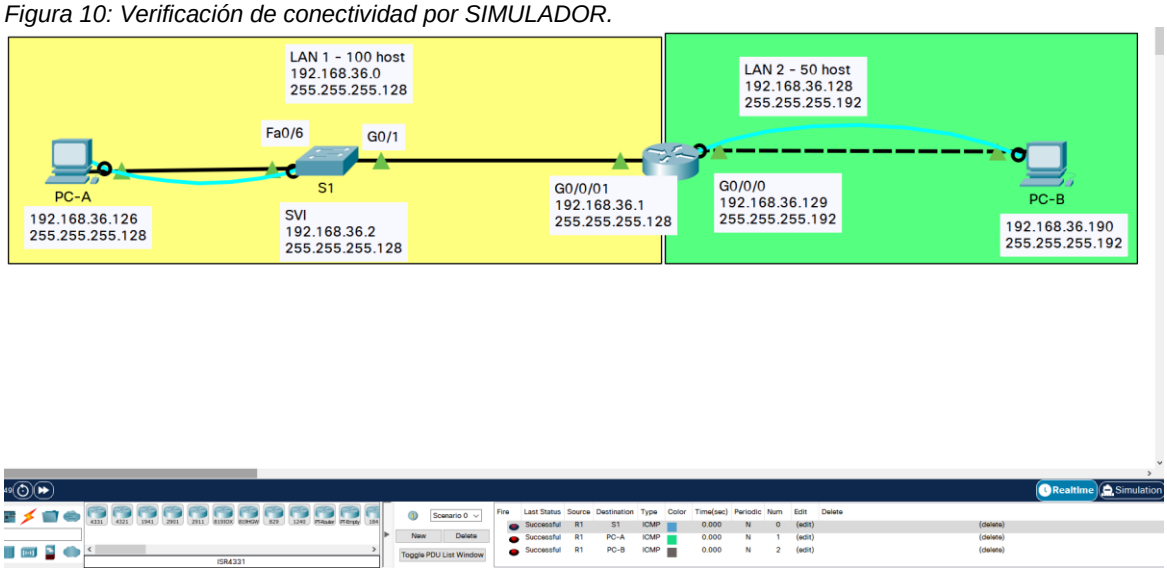


Fuente: Autor.

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

- Prueba de conectividad con el simulador:

Figura 10: Verificación de conectividad por SIMULADOR.



Fuente: Autor.

Verificamos igualmente que tenemos total conectividad entre los diferentes dispositivos de nuestra red.

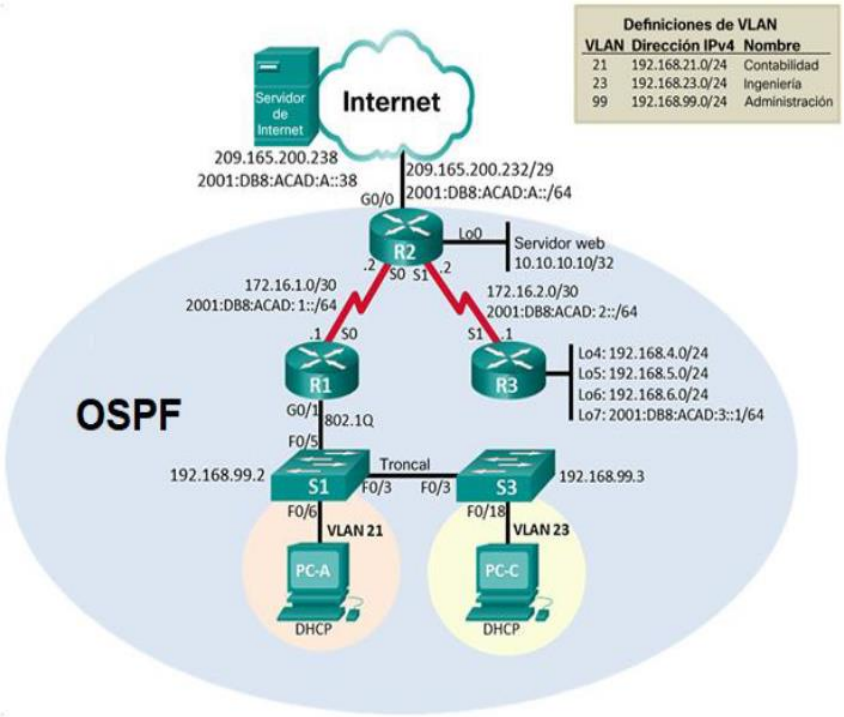
DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

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

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	De esta manera borramos toda la configuración del dispositivo: erase startup-config
Volver a cargar todos los routers	Reiniciamos el dispositivo: Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Borramos la configuración en ejecución y ademas aliminamos 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	De esta manera verificamos que la base de datos no existe en la flash show flash

- Verificamos que la base de datos de la VLAN no esté en el dispositivo.

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: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

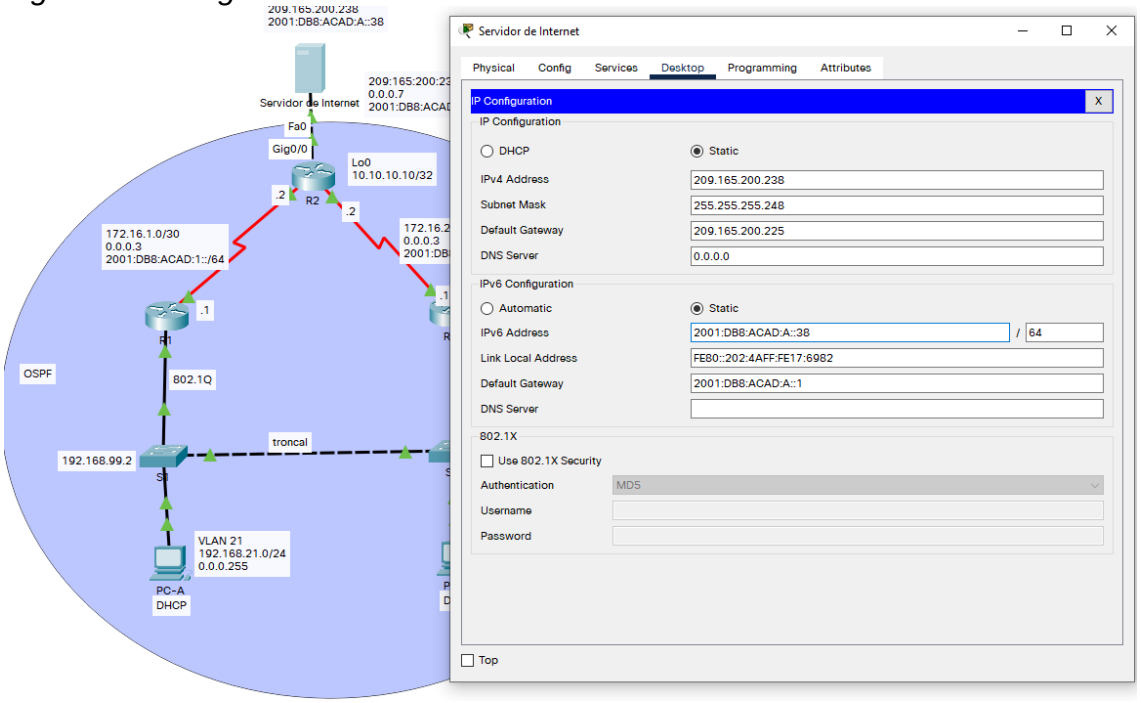
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

En esta sección debemos recordar que el mismo ejercicio nos suministra las direcciones IP que debemos configurar en los diferentes dispositivos:

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

Tabla 1 – configuración PC – internet.

Figura 3 - configuración PC-internet.



Fuente: Autor

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	Desactivamos la búsqueda DNS, de esta manera logramos ahorrar recursos. No ip domain lookup
Nombre del router	Debemos identificar nuestro dispositivo, de esta manera aseguramos su fácil reconocimiento. Hostname R1
Contraseña de exec privilegiado cifrada	Configuramos nuestras contraseñas. 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	Aplicando este comando logramos que las contraseñas se almacenen en texto cifrado y se evita que sean capturados fácilmente. Service password-encyption

Mensaje MOTD	Creamos un mensaje, de esta manera podemos indicar a las personas que quieren ingresar sin autorización de las posibles consecuencias que esto traería: Banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/0	Establezca la descripción
	Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones
	Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones
	Establecer la frecuencia de reloj en 128000
	Activar la interfaz
	
	`interface Serial0/0/0`
	` description Connection to R2`
	` ip address 172.16.1.1 255.255.255.252`
	` ipv6 address 2001:DB8:ACAD:1::1/64`

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0
	Configurar una ruta IPv6 predeterminada de S0/0/0
	
	`ip route 0.0.0.0 0.0.0.0 Serial0/0/0`
	`!`
	`ip flow-export version 9`
	`!`
	`ipv6 route ::/0 Serial0/0/0`

Tabla 2 – configuración R1.

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Desactivamos la búsqueda DNS y evitamos que recursos se empleen en actividades innecesarias. No ip domain lookup
Nombre del router	Debemos identificar nuestro dispositivo. Hostname R2
Contraseña de exec privilegiado cifrada	Creamos nuestras contraseñas que nos permite proteger nuestros equipos: Enable secret class
Contraseña de acceso a la consola	Creamos las contraseñas del puerto de CONSOLA: Line console 0 Password cisco Login
Contraseña de acceso Telnet	Creamos las contraseñas de las lineas virtuales VTY: Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Debemos proceder a encriptar las contraseñas: Service password-encyption

Habilitar el servidor HTTP	ip http server
	
	Este comando no es soportado por packet tracer. Por este motivo optamos por instalar un servidor.
	
	`R2(config)#`
	`R2(config)#ip http server`
	`^`
	`% Invalid input detected at '^' marker.`
	
	`R2(config)#`

Mensaje MOTD	Cremos un mensaje de bienvenida en los dispositivos el cual aparece inmediatamente querramos ingresar a un dispositivo en particular. Banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/0	Establezca la descripción
	Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.
	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
	Activar la interfaz
	
	`interface Serial0/0/0`
	` 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`

Interfaz S0/0/1	Establecer la descripción
	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
	Establecer la frecuencia de reloj en 128000.
	Activar la interfaz
	
	`interface Serial0/0/1`
	` 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`

Interfaz G0/0 (simulación de Internet)	Establecer la descripción.
	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
	Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.
	Activar la interfaz
	
	`interface GigabitEthernet0/0`
	` description Connection to Internet`
	` ip address 209.165.200.233 255.255.255.248`
	` ip nat outside`
	` duplex auto`
	` speed auto`
	` ipv6 address 2001:DB8:ACAD:A::1/64`

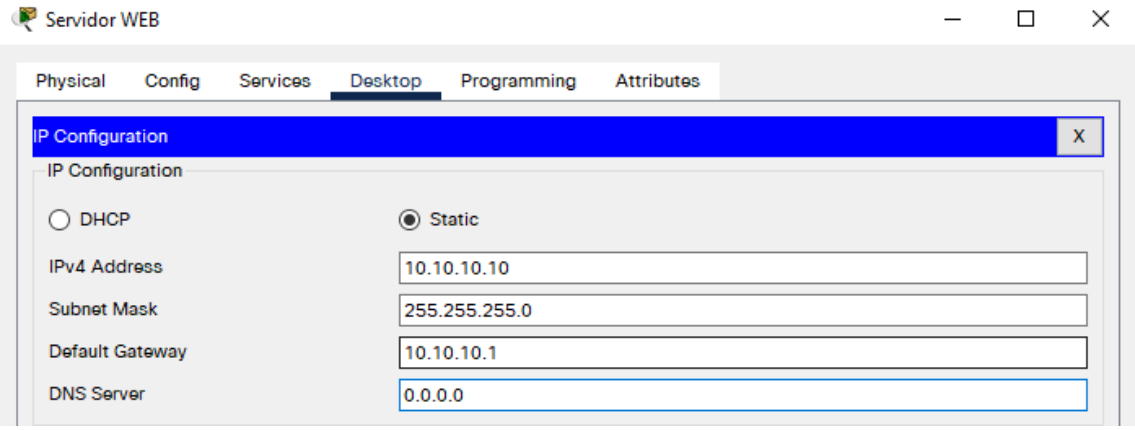
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción.
	Establezca la dirección IPv4.
	
	`R2#config`
	`Configuring from terminal, memory, or network [terminal]?`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`R2(config)#`
	`R2(config)#int g0/1`
	`R2(config-if)#ip addres 10.10.10.1 255.255.255.0`
	`R2(config-if)#no shutdown`

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0.
	Configure una ruta IPv6 predeterminada de G0/0.
	
	`ip classless`
	`ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0`
	`!`
	`ip flow-export version 9`
	`!`
	`ipv6 route ::/0 GigabitEthernet0/0`

Tabla 3 – configuración R2.

- Configuración del servidor WEB.

Figura 4 - configuración del servidor WEB.



Fuente: Autor

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Desactivamos la busqueda DNS ahorrando recursos: No ip domain lookup
Nombre del router	Debemos identificar los dispositivos. Hostname R3
Contraseña de exec privilegiado cifrada	Configuramos las diferemtes contraseñas. Enable secret class
Contraseña de acceso a la consola	Configuramos en este caso la contraseña de la interfaz: Line console 0 Password cisco login
Contraseña de acceso Telnet	Configuramos las contraseñas de las lineas virtuales: Line vty 0 4 Password cisco login
Cifrar las contraseñas de texto no cifrado	Procedemos a encriptar nuestras contraseñas: Service password-encyption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Interfaz S0/0/1	Establecer la descripción
	Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.
	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
	Activar la interfaz
	
	`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`

Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback4 Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred. Interface loopback5 Ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred. Interface loopback6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones. Interface loopback7 Ipv6 address 2001:DB8:ACAD:3::1/64

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

Tabla 4 – configuración R3.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Procedemos a desactivar la busqueda 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-encyption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Tabla 5 – configuración S1.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
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-encyption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Tabla 6 – configuración S3.

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	172.16.2.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

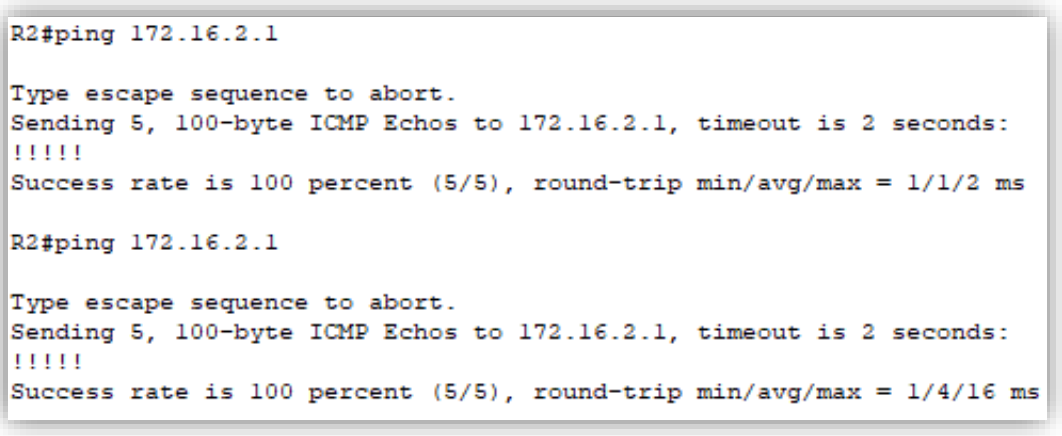
Tabla 7 – prueba de conectividad.

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: Autor

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: Autor

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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
	
	`interface Vlan99`
	`ip address 192.168.99.2 255.255.255.0`
	
	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` 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`
	
	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 int range fastethernet 1-2, fa0/4, fa0/6-24, g1/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	Empleamos el siguiente comando 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

Tabla 8 – configuración interfaces S1

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación

Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
	
	Interface vlan 23
	
	`interface FastEthernet0/18`
	` 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
	
	`interface Vlan99`
	` 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	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

Tabla 9 – configuración interfaces S3

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/1.21 description Accounting LAN encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/1.23 description Accounting LAN encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/1.99 description Accounting LAN encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	interface g0/1 no shutdown

Tabla 10 – configuración interfaces R1

Paso 4: Verificar la conectividad de la red

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

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

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

Tabla 11 – prueba de conectividad desde los ROUTERS

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: Autor

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: Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

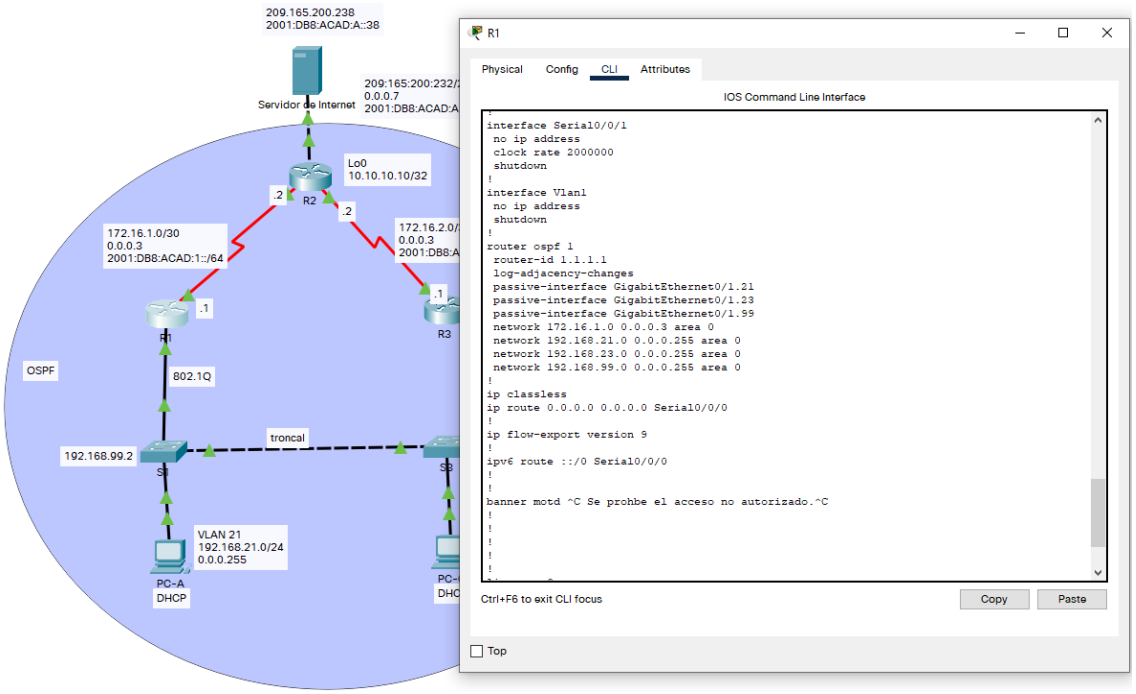
Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	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
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

Tabla 12 – configuración de OSPF en R1

Figura 9 - Configurar OSPF en el R1



Fuente: Autor

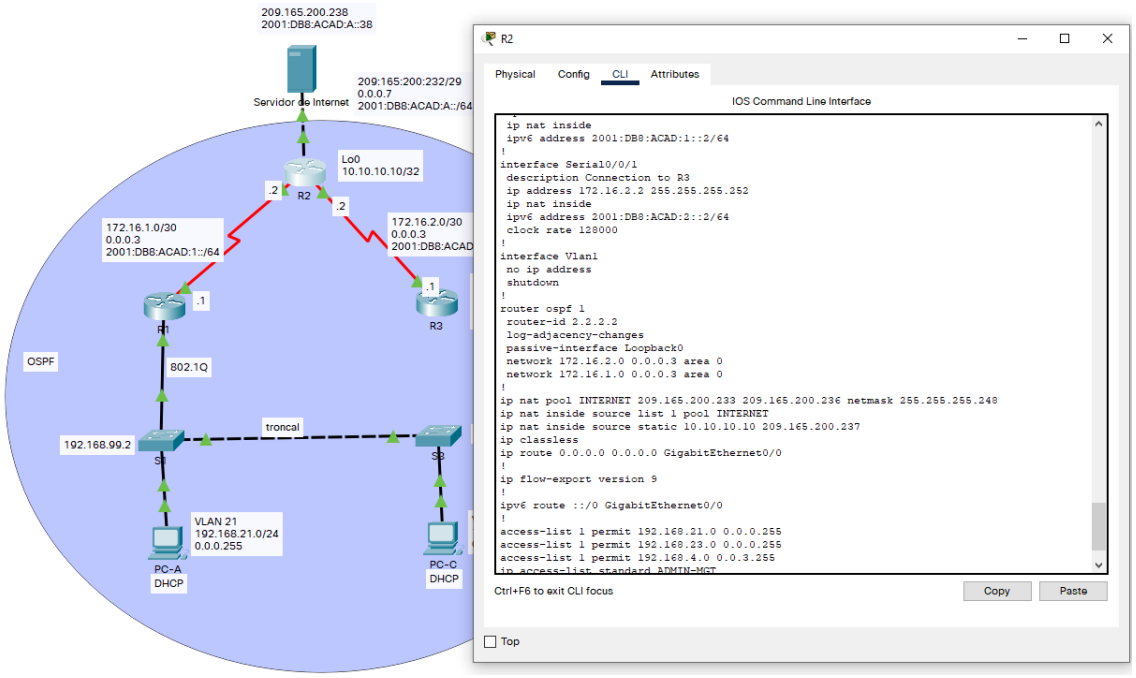
Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#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	passive-interface lo0 passive-interface g0/1
Desactive la sumarización automática.	no auto-summary

Tabla 13 – configuración de OSPF en R2

Figura 10 - Configurar OSPF en el R2



Fuente: Autor

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

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	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	passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	no auto-summary

Tabla 14 – configuración de OSPF en R3

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
R3(config-router)#
R3(config-router)#do wr
```

Fuente: Autor

Paso 4: Verificar la información de OSPF

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

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

Tabla 15 – comandos de verificación de OSPF.

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: Autor.

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: Autor.

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: Autor

Parte 5: Implementar DHCP y NAT para IPv4

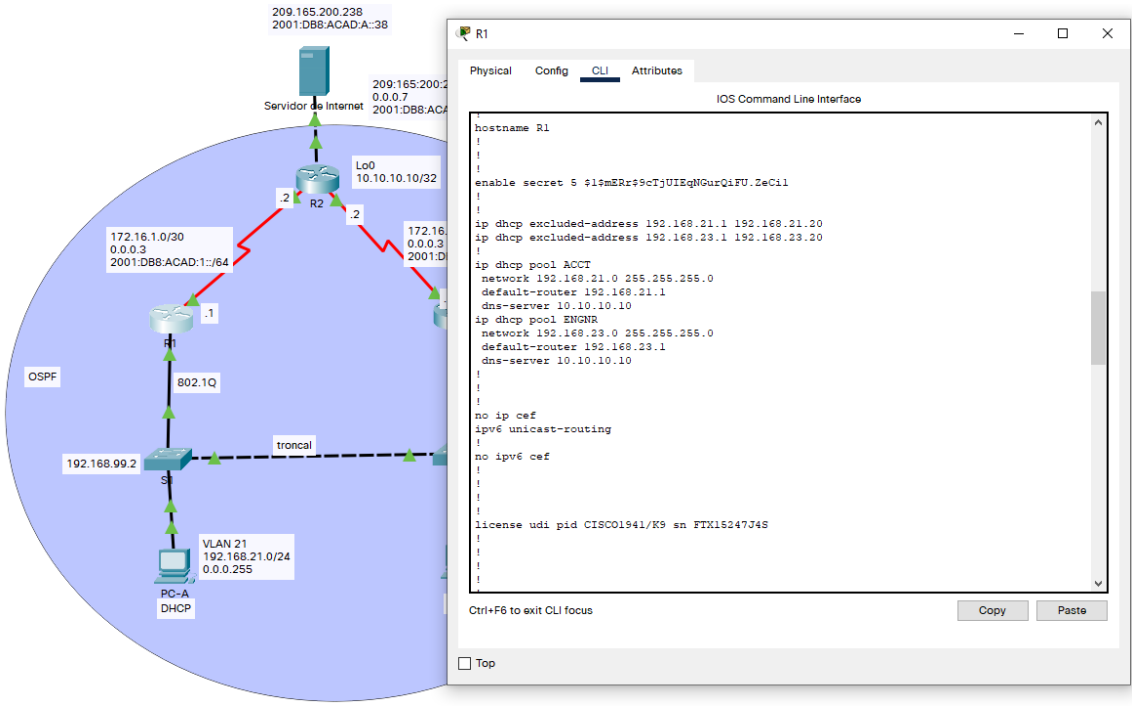
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	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	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado 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
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado 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

Tabla 16 – configuración de DHCP.

Figura 15 - Implementar DHCP y NAT para IPv4



Fuente: Autor.

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

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

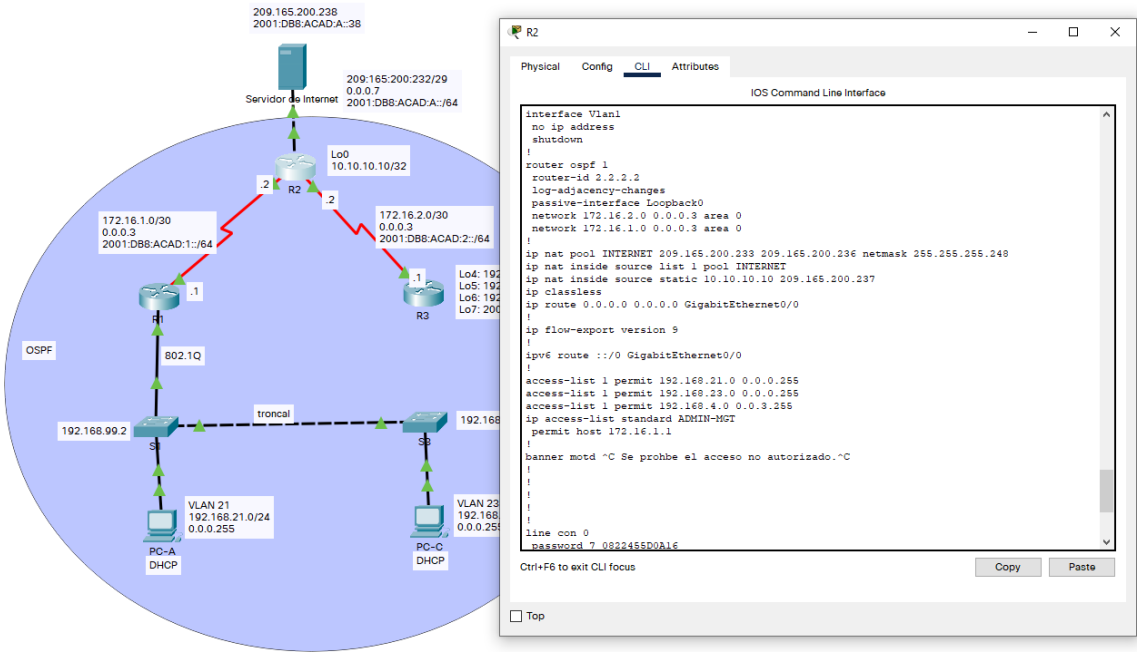
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** User webuser privilege 15 secret cisco 12345

Habilitar el servicio del servidor HTTP	ip http server este commando no es soportado por packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local packet tracer no soporta este commando
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** Ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	interface g0/0 ip nat outside interface g0/1 ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 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
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228** Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Definir la traducción de NAT dinámica	Hacemos el NAT dinamico con el fin de poder hacer la tradución empleando la lista 1. ip nat inside source list 1 pool INTERNET

Tabla 17 – configuración NAT estático Y dinámico.

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



Fuente: Autor

Paso 3: Verificar el protocolo DHCP y la NAT estática

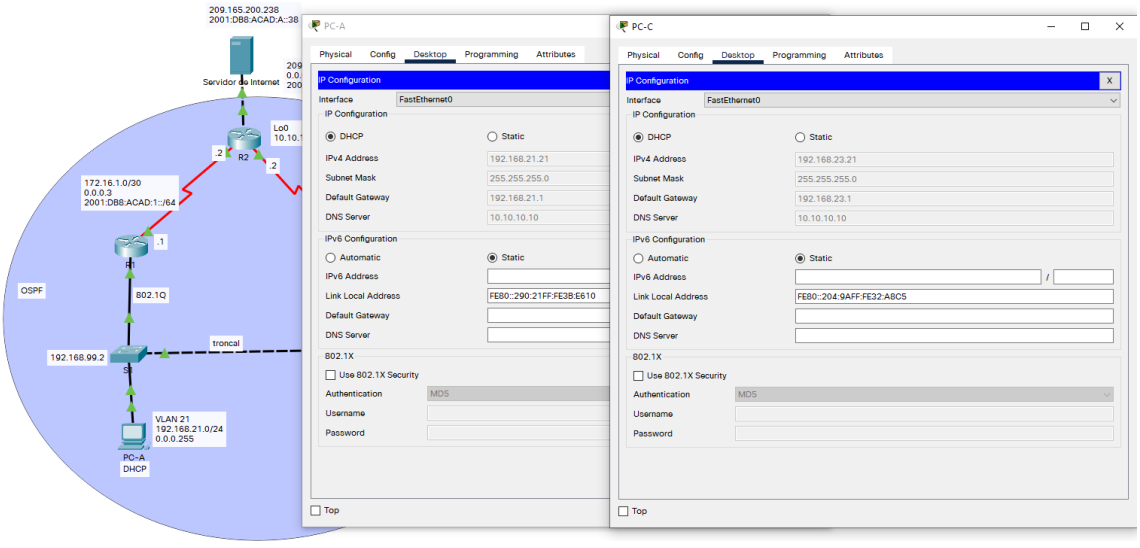
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	C:\>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
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	C:\>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

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	C:\>ping 192.168.23.21 Pinging 192.168.23.21 with 32 bytes of data: Request timed out. Reply from 192.168.23.21: bytes=32 time=1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1ms TTL=127 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
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 **webuser** y la contraseña **cisco12345**	Exitoso.

Tabla 18 – verificación de DHCP y NAT.

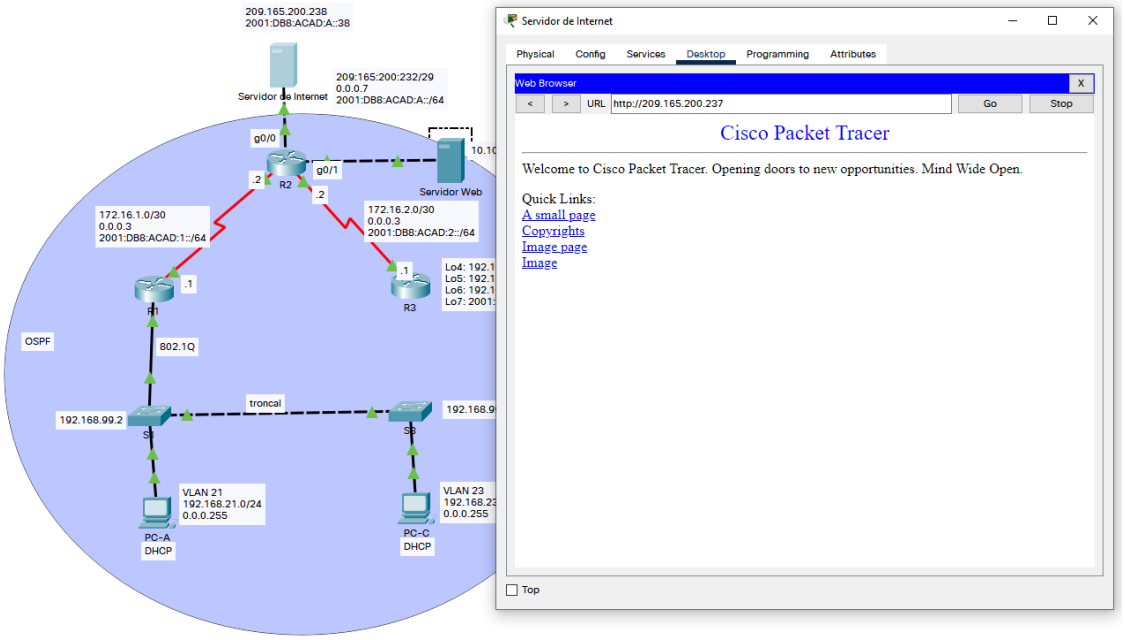
Figura 17 - verificación de DHCP.



Fuente: Autor

- Acceso al servidor web desde el PC Internet

Figura 18 - verificación servicio WEB.



Fuente: Autor

Parte 6: Configurar NTP

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

Tabla 19 – NTP

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

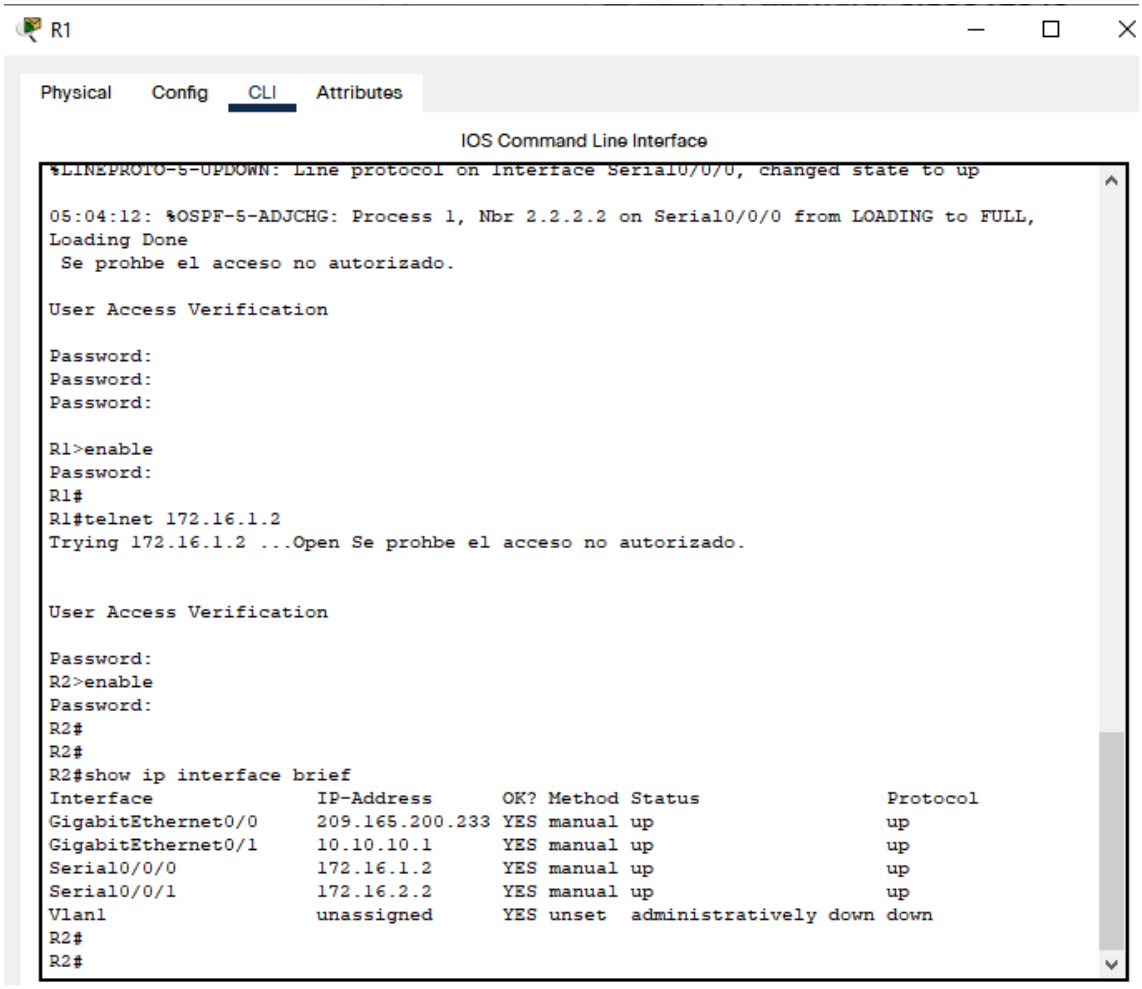
Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** 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#

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

- TELNET desde RI a R2

Figura 19 - TELNET desde R1 a R2



Fuente: Autor

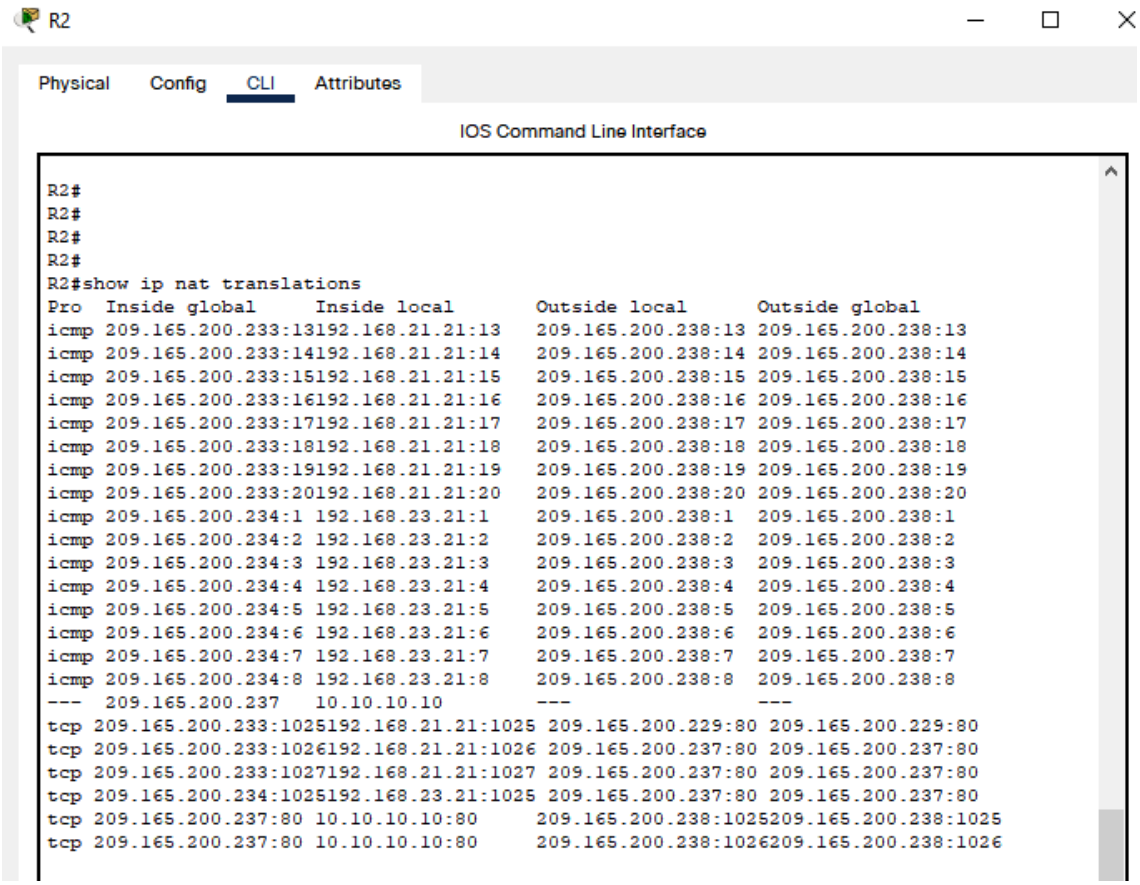
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	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#
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
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. Show ip nat translation Show ip nat statics
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

Tabla 21 – comando SHOW.

- Verificamos las traducciones NAT en R2.

Figura 20 - verificación de NAT.



Fuente: Autor

CONCLUSIONES

Hemos interiorizado muchos de los aspectos tratados a lo largo de nuestra carrera y del diplomado, aspectos tales como la configuración de dispositivos, aspectos que nos suministrar muchas destrezas.

Comprendo la diferencia que existe en la configuración del direccionamiento IPV6 como IPV4 además de toso el proceso de configuración que conlleva cada uno de ellos.

Finalmente, en este escenario identificamos y solucionamos el problema propio de enrutamiento mediante el uso adecuado de estrategias basadas en comandos IOS y de tráfico en las interfaces.

Comprendo el proceso de configuración de VLAN y su importancia a la hora de segmentar las redes de una manera virtual, todo esto con el fin de organizar mucho mejor.

Comprendo la importancia de las contraseñas y sus variantes a la hora de configurarlos dentro de los dispositivos.

Comprendo la importancia de la configuración de los protocolos de enrutamiento, para nuestro caso el protocolo OSPF, gracias al cual es posible el enrutamiento de paquetes dentro de la red

BIBLIOGRAFIA

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

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

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

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

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

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

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