# SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO.

JOHN JAIRO RAMIREZ GUEVARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-PASTO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
CIUDAD: JAMUNDI
NOVIEMBRE DEL 2020

# SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO.

JOHN JAIRO RAMIREZ GUEVARA

ASESOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-PASTO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
CIUDAD: JAMUNDI
NOVIEMBRE DEL 2020

Ciudad: JAMUNDI (Valle.) Noviembre del 2020.

Nota de aceptación.

_____
_____
_____
_____
_____

Firma del Jurado.

Firma del Jurado.

Este logro en mi vida profesional va dedicado a mi familia, mi esposa e hija quienes me han acompañado y dado la fortaleza para continuar en momentos que perdía la motivación. También a mi madre, que, aunque no ya no está con nosotros siempre me incentivo a seguir estudiando y buscar nuevas oportunidades

_____

JOHN JAIRO RAMIREZ GUEVARA.

## AGRADECIMIENTOS

Este es un día de gran importancia dentro de mi vida, en el cual expreso mis agradecimientos a:

Antes que nada, agradezco a Dios y a mis padres por concederme la vida y hacer posible el mejorar constantemente, agradezco a mis abuelos, tíos, hermanos, suegros, esposa e hijos y a todas las personas que directa o indirectamente han tenido a ayudarme en este camino, apoyándome con sus palabras y acompañamiento para mi formación como ser humano y profesional, en respuesta a esto, cuenten con un gran amigo.

Le agradezco a la Universidad Nacional Abierta y a Distancia UNAD, por ser una de las instituciones más prestigiosas y por brindarme esa posibilidad de formarme como profesional y poderle servir a mí comunidad.

Les agradezco también a los Docentes, los cuales nos han acompañado a lo largo de todo nuestro proceso formativo.

## TABLA DE CONTENIDO

# Lista de figuras

# Lista de Tablas

## RESUMEN

En la presente actividad se va a desarrollar una solución para dos escenarios Corporativos en el cual aplicaremos la temática y nuestras destrezas relacionados con las redes y las telecomunicaciones, comenzaremos con toda la parte del diseño de la TOPOLOGIA con el fin de conocer la forma como los dispositivos va a estar conectados, sus interfaces y de esta manera conoce las subredes y la distribución de os equipos de entro de cada una de ellas, Por otra parte se continuará con la configuración de cada uno de los dispositivos que intervienen, PC, switches, routers, servidores, etc., todo ellos indicando desde la configuración más básica hasta aplicar los comandos que me permiten el intercambio de paquetes y la seguridad dentro de mi red.



Palabras clave: OSPF, RIP, Router, Switch, VLSM.



ABSTRACT:

In this activity, we will develop a solution for two Corporate scenarios in which we will apply the theme and our skills related to networks and telecommunications, we will begin with the entire design part of the TOPOLOGY in order to know how the devices will be connected, their interfaces and in this way you know the subnets and the distribution of the equipment inside each one of them. On the other hand, we will continue with the configuration of each of the devices involved, PCs, switches, routers, servers, etc., all of them indicating from the most basic configuration to applying the commands that allow me to exchange packets and security within my network.

# INTRODUCCION

Como profesionales de las ramas de la ingeniería es de vital importancia poder practicar los conocimientos que hemos adquirido a lo largo de nuestra carrera y del Diplomado en el desarrollo de ESCENARIOS que nos exijan poner en práctica todas esas habilidades adquiridas. Es elemental para nuestra vida el hecho de poner en práctica cada uno de nuestros conocimientos, y más aún cuando este va encaminado a dar solución a inconvenientes que se presentan en nuestras sociedades.

La tecnología es mucho más asequible en nuestros días, por lo cual todos no importando muchas veces las clases sociales podemos estar inmersos dentro de su mundo, en nuestras vidas la tecnología ya es parte esencial para su correcto desarrollo
Ya no solo se tiene un ordenador para satisfacer todas las necesidades de cálculo de una organización, se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Son muchas las tecnologías que están avanzando a pasos agigantados, pero lo cierto es que debemos adaptarnos a esos cambios, y más como profesionales estar a la vanguardia de la misma y así poder brindar las mejores tecnologías a nuestra población.

A través de CISCO NETWORKING, en convenio con la Universidad Nacional Abierta y a Distancia, se pudo trabajar en dos módulos de redes LAN – WAN y CONFIGURACION DE ROUTERS, los cuales se fueron desarrollando de acuerdo al cronograma generado y de fácil acceso para todos. Desarrollaremos entonces 2 ESCENARIOS en los cuales configuraremos una serie de necesidades de las diferentes organizaciones.

# 1. JUSTIFICACIÓN.

Cuando ingresamos a la UNIVERSIDAD una de las metas que teníamos planteadas es la superación ser excelentes profesionales y de esta manera poder brindarle a nuestra comunidad la posibilidad de acceder igualmente a ese conocimiento. Debemos ser conscientes de lo amplio del tema que manejamos y lo debemos hacer a la perfección.

Las ingenierías hacen parte de todos los campos de nuestras sociedades La Ingeniería es una de las ramas que más se ha expandido, en todo lado vemos funcionando redes, dependemos de ella en nuestro trabajo, por diversión, para podernos comunicar entre muchas otras funciones más. Las redes nos facilitan las cosas.

Por esto nuestra intención es que pongamos en práctica todo lo que se ha aprendido, y que mejor manera que a través de la implementación de un caso real, donde midamos nuestros conocimientos y aptitudes desarrollados durante el curso.

# 2. OBJETIVOS

## 2.1 OBJETIVO GENERAL

Poner en práctica lo aprendido a lo largo de nuestra carrera y del Diplomado en el desarrollo de 2 ESCENARIOS reales, realizando la implementación de cada una de estas redes siguiendo unas exigencias preestablecidas. Posterior a esto, estos deben ser montados y configurados con la ayuda del simulador de red PACKET TRACERT, además deberemos documentando cada uno de los pasos que se desarrollaron para alcanzar el objetivo.

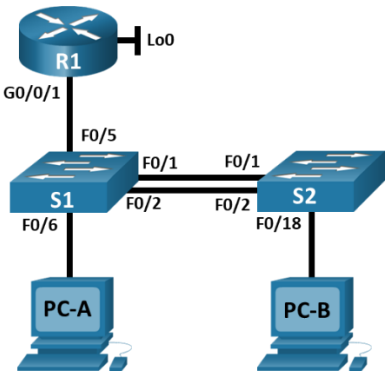
## 2.2 OBJETIVOS ESPECÍFICOS

- Profundizar en el manejo de la herramienta de PACKET TRACER.
- Diseñar y documentar el Esquema de direccionamiento que vamos a emplear dentro de la red.
- Aplicar la configuración a cada uno de los dispositivos de acuerdo a las exigencias indicadas.
- Verificar la conectividad entre todos los dispositivos de la topología de la red.
- Comprender el funcionamiento de cada uno de los dispositivos que intervienen.

# 3. ESCENARIO 1

## 3.1 TOPOLOGIA

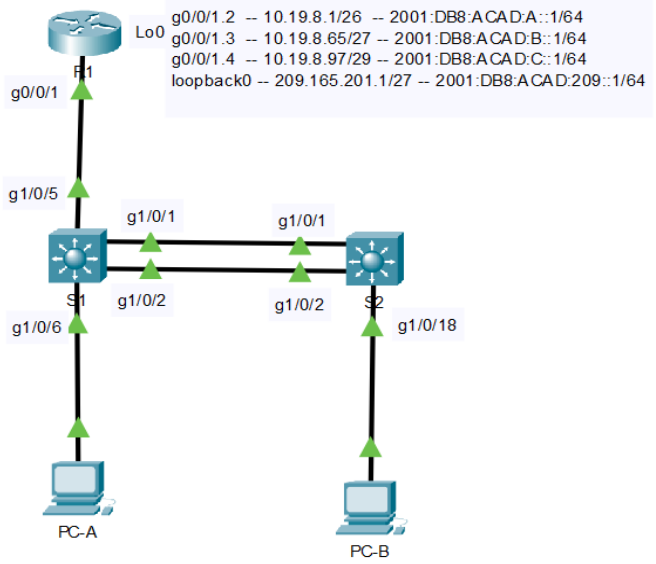
**Figura 1 – Topología del escenario I.**




Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

**Figura 2 -Topología del escenario 2 en PKT**

Asignación de interfaces y sub. Interfaces, vista general de la topología.




Fuente Autor.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, EtherChannel y port-security.

**Tabla 1 - VLANS.**

| VLAN | Nombre de la VLAN |
|---|---|
| 2 | Bikes |
| 3 | Trikes |
| 4 | Management |
| 5 | Parking |
| 6 | Native |

**Tabla 2 – Lista de direccionamiento.**

| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|---|---|---|
| R1 G0/0/1.2 | 10.19.8.1 /26 | No corresponde |
| R1 G0/0/1.2 | 2001:db8:acad:a: :1 /64 | No corresponde |
| R1 G0/0/1.3 | 10.19.8.65 /27 | No corresponde |
| R1 G0/0/1.3 | 2001:db8:acad:b: :1 /64 | No corresponde |
| R1 G0/0/1.4 | 10.19.8.97 /29 | No corresponde |
| R1 G0/0/1.4 | 2001:db8:acad:c: :1 /64 | No corresponde |
| R1 G0/0/1.6 | No corresponde | No corresponde |
| R1 Loopback0 | 209.165.201.1 /27 | No corresponde |
| R1 Loopback0 | 2001:db8:acad:209: :1 /64 | No corresponde |
| S1 VLAN 4 | 10.19.8.98 /29 | 10.19.8.97 |
| VLAN S1 4 | 2001:db8:acad:c: :98 /64 | No corresponde |
| S1 VLAN 4 | fe80: :98 | No corresponde |
| S2 VLAN 4 | 10.19.8.99 /29 | 10.19.8.97 |
| S2 VLAN 4 | 2001:db8:acad:c: :99 /64 | No corresponde |
| S2 VLAN 4 | fe80: :99 | No corresponde |

| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|---|---|---|
| PC-A NIC | Dirección DHCP para IPv4 | DHCP para puerta de enlace predeterminada IPv4 |
| PC-A NIC | 2001:db8:acad:a: :50 /64 | fe80::1 |
| PC-B NIC | DHCP para dirección IPv4 | DHCP para puerta de enlace predeterminada IPv4 |
| PC-B NIC | 2001:db8:acad:b: :50 /64 | fe80::1 |

**Nota**: No hay ninguna interfaz en el router que admita VLAN 5.

## 3.2 INSTRUCCIONES

Paso 1: Inicializar y volver a cargar el router y el switch, borrando las configuraciones de inicio y las VLAN del router y los switch y cargando de nuevo los dispositivos. Con esto se evitará conflictos al conectar los dispositivos.

**Tabla 3 - inicialización de los dispositivos.**

| Tarea | Especificación de comandos |
|---|---|
| En este caso vamos a borrar la configuración del Switch y procederemos a cargar nuevamente cada uno de los dispositivos.<br>Debemos confirmas que se desea reiniciar cada dispositivo. | **S1**<br>Erase-startup-config<br>Delete vlan.dat<br>Reload<br>**S2**<br>Erase-startup-config<br>Delete vlan.dat<br>Reload |

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

**Tabla 4 - Inicialización de los dispositivos.**

| Tarea | Especificación |
|---|---|
| Configuración de tablas SDM la cual nos permite sacar un mayor provecho a los dispositivos. | **Figura 3 – SDM activa.**<br>Switch(config)# sdm prefer dual-ipv4-and-ipv6 default<br>Switch(config)# exit<br>Switch# reload<br>Proceed with reload? [confirm]<br>Fuente: autor. |

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Paso 2: A continuación se realiza la configuración del router R1 dispositivo que al cual le vamos a configurar una serie de parámetros básicos para su funcionamiento, lo primero desactivar la búsqueda DNS esto con el fin de ahorrar recursos, configuramos el nombre del dispositivos, aspecto muy importante para conocer exactamente en el dispositivo que nos encontramos, configuramos los dominios según la tabla indicada, se configura todos los aspectos de seguridad y además cifamos las mismas con el fin de que no sean capturadas fácilmente, configuramos el mensaje que aparece cada vez que se intenta ingresar al mismo y por último con la ayuda de la tabla de direccionamiento que se nos suministra terminamos configurando las interfaces y subinterfaces

**Tabla 5 - Configuracion basica - R1**

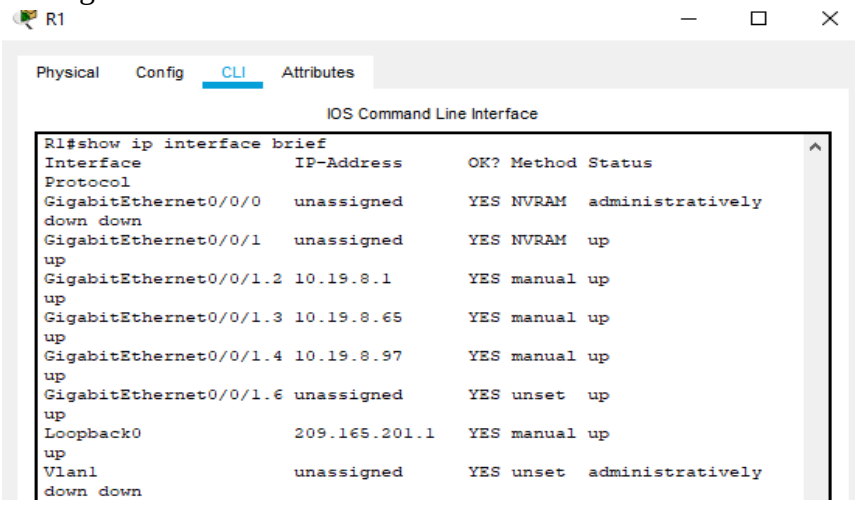
| Tarea | Especificación de comandos |
|---|---|
| Desactivar la búsqueda DNS | No ip domain-lookup |
| Nombre del router | Hostname R1 |
| Nombre de dominio | En modo de configuración se coloca el comando para asignarle el nombre de dominio así:<br>ccna-lab.com<br>ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado<br><br>Ciscoenpass<br>Enable secret ciscoenpass |

| Tarea | Especificación de comandos |
|---|---|
| Contraseña de acceso a la consola | En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola<br>Ciscoconpass<br>Line console 0<br>Password ciscoconpass<br>Login |
| Establecer la longitud mínima para las contraseñas | En modo de configuración se coloca el comando para que se establezca la longitud mínima para las contraseñas de 10 caracteres<br>Security passwords min-leng 10 |
| Crear un usuario administrativo en la base de datos local | En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre:<br>Username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | En modo de configuración se coloca el comando para configurar el inicio de sesión en las líneas VTY<br>Line vt 0 15 login local |
| Configurar VTY solo aceptando SSH | En modo de configuración se coloca el comando para configurar VTY solo para que acepte SSH<br>Transport input ssh |
| Cifrar las contraseñas de texto no cifrado | Encriptamos las contraseñas con el fin de que no queden almacenadas en texto plano.<br>Service password-encryption |
| Configure un MOTD Banner | Creamos nuestro mensaje del dispositivo<br>Banner motd & acceso no autorizado & |
| Habilitar el routing IPv6 | Habilitamos IPV6.<br>Ipv6 unicast-routing |

| Tarea | Especificación de comandos |
|---|---|
| Configurar interfaz G0/0/1 y subinterfaces | Establezca la descripción<br>Establece la dirección IPv4.<br>Establezca la dirección local de enlace IPv6 como **fe80: :1**<br>Establece la dirección IPv6.<br>Activar la interfaz.<br>Int g0/0/1.2<br>Encapsulation dot1q 2<br>Description BIKES<br>Ip addres 10.19.8.1 255.255.255.192<br>Ipv6 addres 2001:db8:acad:a:1/64<br>Ipv6 addres fe80::1 link local<br>Int g0/0/1<br>No shutdown<br>Int g0/0/1.3<br>Encapsulation dot1q 3<br>Description TRIKES<br>Ip addres 10.19.8.65 255.255.255.224<br>Ipv6 addres 2001:db8:acad:b:1/64<br>Ipv6 addres fe80::1 link local |

**Figura 4 - Configuración**

Evidencia IPs Configuradas en el CLI del router

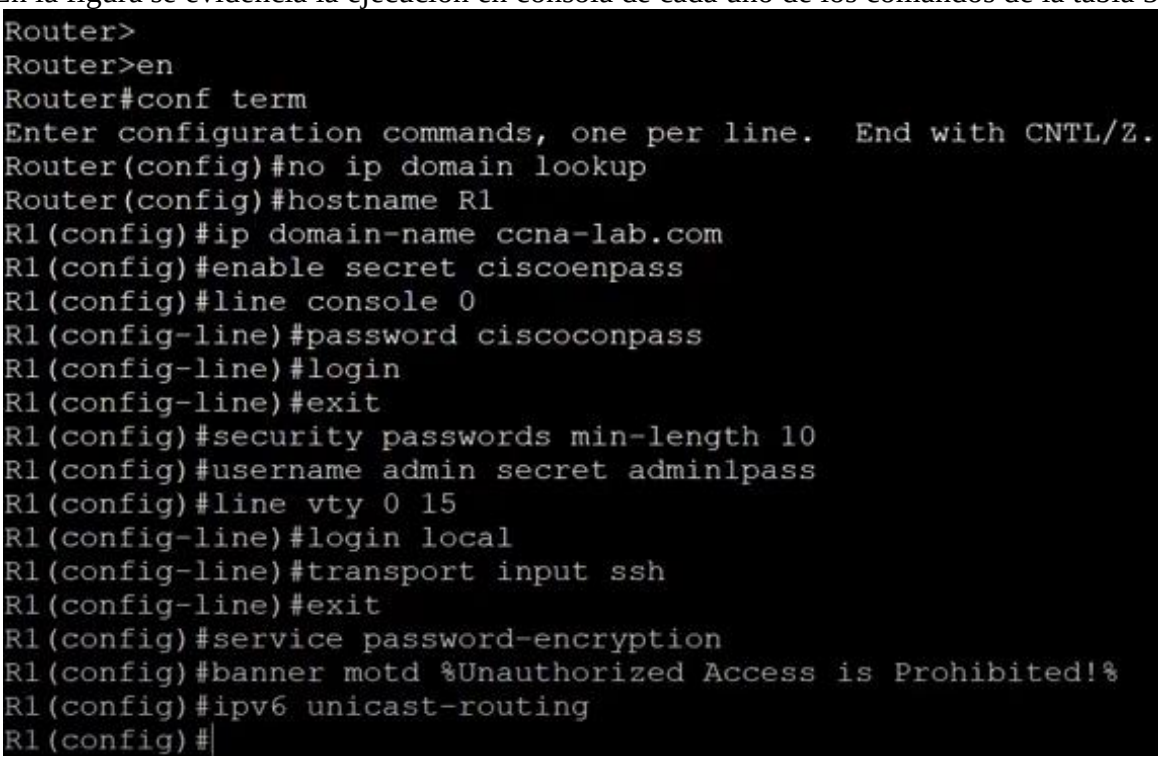



Fuente Autor.

| Tarea | Especificación de comandos |
|---|---|
| Configurar interfaz G0/0/1 y subinterfaces | Int g0/0/1.4<br>Encapsulation dot1q 4<br>Description MANAGEMENT<br>Ip addres 10.19.8.97 255.255.255.224<br>Ipv6 addres 2001:db8:acad:c:1/64<br>Ipv6 addres fe80::1 link local<br><br>Int g0/0/1.6<br>Encapsulation dot1q 6 NARIVE<br>Description NATIVE<br>Ip addres 10.19.8.97 255.255.255.224<br>Ipv6 addres 2001:db8:acad:c:1/64<br>Ipv6 addres fe80::1 link local<br><br>Int g0/0/1<br>No shutdown |
| Configure el Loopback0 interface | Establezca la descripción<br>Establece la dirección IPv4.<br>Establece la dirección IPv6.<br>Establezca la dirección local de enlace IPv6 como **fe80::1**<br><br>Interface loopback 0<br>Ip address 209.165.201.1 255.255.255.224<br>Ipv6 address 2001:db8:acad:209::1/64<br>Ipv6 address fe80::1 link-local<br>Description INTERNET |
| Generar una clave de cifrado RSA | Módulo de 1024 bits<br>Crypto key generate rsa modulus 1024 |

**Figura 5 - Config R1, nombre, contraseñas, banner.**

En la figura se evidencia la ejecución en consola de cada uno de los comandos de la tabla 5



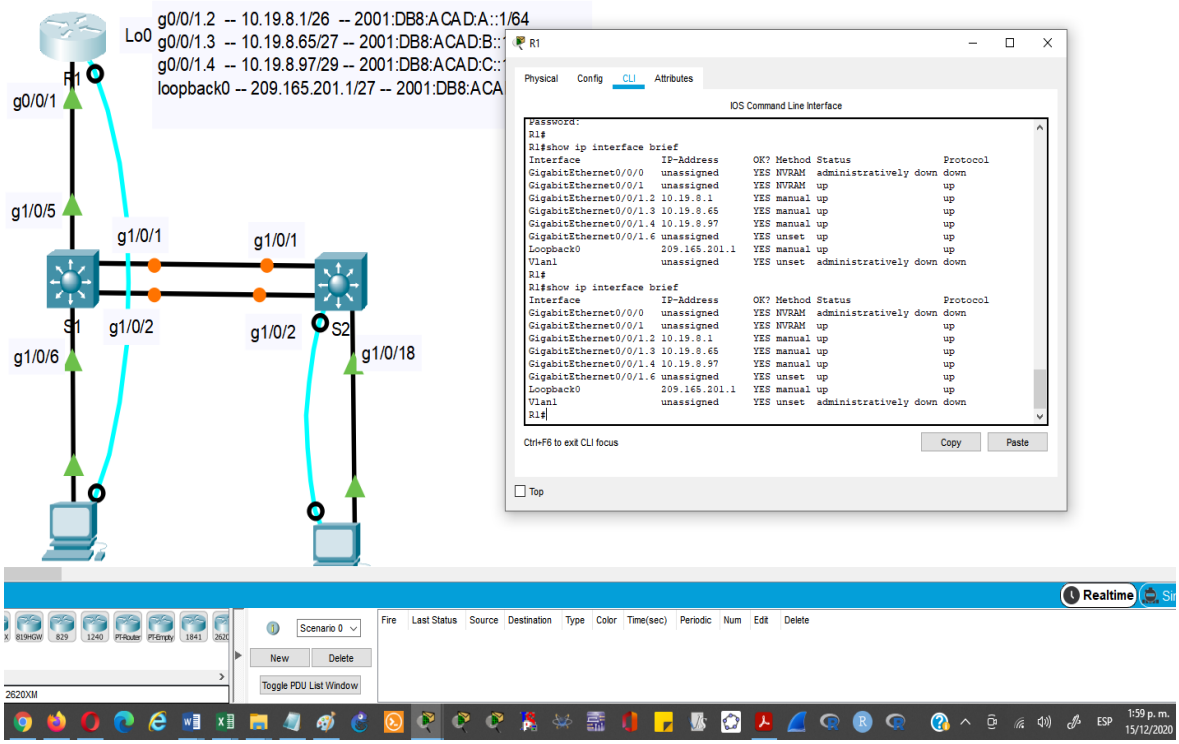

Fuente: autor.

**Tabla 6 – Configuración interfaces R1.**

| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|---|---|---|
| R1 G0/0/1.2 | 10.19.8.1 /26 | No corresponde |
| R1 G0/0/1.2 | 2001:db8:acad:a: :1 /64 | No corresponde |
| R1 G0/0/1.3 | 10.19.8.65 /27 | No corresponde |
| R1 G0/0/1.3 | 2001:db8:acad:b: :1 /64 | No corresponde |
| R1 G0/0/1.4 | 10.19.8.97 /29 | No corresponde |
| R1 G0/0/1.4 | 2001:db8:acad:c: :1 /64 | No corresponde |
| R1 G0/0/1.6 | No corresponde | No corresponde |
| R1 Loopback0 | 209.165.201.1 /27 | No corresponde |
| R1 Loopback0 | 2001:db8:acad:209: :1 /64 | No corresponde |

**Figura 6 - Configuración de interfaces en R1, verificación.**

Mediante un show interface brief se evidencia como están configuradas las interfaces en R1




Fuente: autor.

Paso 3: Continuamos nuestro proceso de configuración, esta vez con el S1, el proceso es muy similar ya que los parámetros que estamos configurando son los básicos, entonces, desactivamos la búsqueda de DNS de este, configuramos un nombre con el fin de identificarlo. Configuramos el respectivo dominio, configuramos todo lo relacionado con las contraseñas y las encriptamos de una vez, configuramos las líneas VTY y configuramos sus contraseñas, agregamos el mensaje BANNER MOTD que es el que aparece cada vez que queremos ingresar al dispositivo configuramos las VLAN y el Gateway predeterminado

**Tabla 7 – Configuración Básica SWITCH 1.**

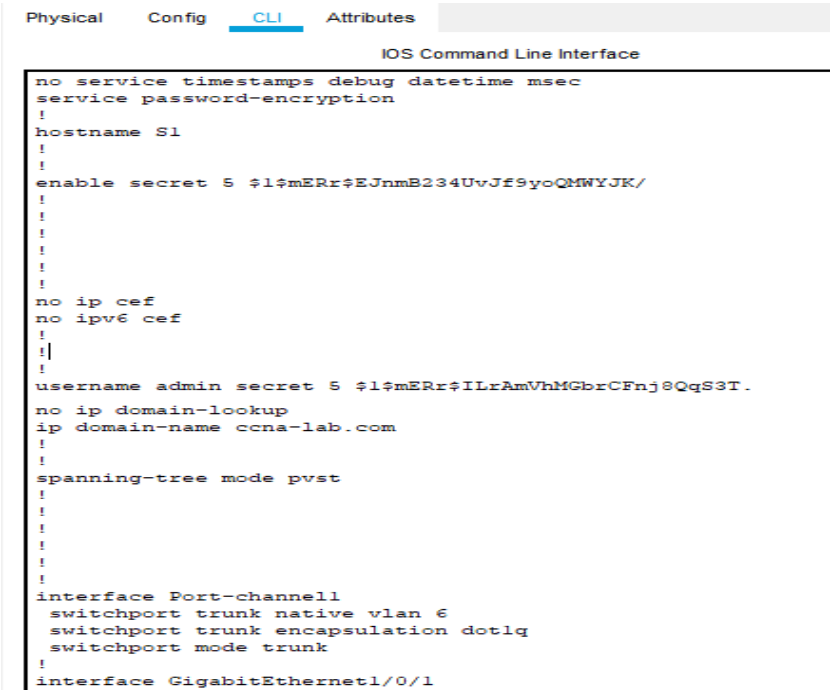
| Tarea | Especificación de Comandos |
|---|---|
| Desactivar la búsqueda DNS. | Procedemos a aplicar el comando indicado, esto con el fin de desactivar la búsqueda DNS<br><br>No ip domain lookup |
| Nombre del switch | Debemos identificar nuestros dispositivos, esto con el fin de identificarlos fácilmente el dispositivo que estamos configurando, para ello empleamos el siguiente comando en cada uno de los dispositivos.<br><br>**S1 o S2, según proceda.**<br><br>Hostname S1<br>Hostname S2 |
| Nombre de dominio | En modo de configuración se coloca el comando para asignarle el nombre de dominio así:<br><br>**ccna-lab.com**<br><br>ip domain name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado<br><br>**Ciscoenpass**<br>Enable secret ciscoenpass |
| Contraseña de acceso a la consola | En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola así:<br><br>**Ciscoconpass**<br>Line console 0<br>Password ciscoconpass<br>Login |

| Tarea | Especificación de Comandos |
|---|---|
| Crear un usuario administrativo en la base de datos local | En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre:<br><br>Nombre de usuario: **admin**<br>Password: **admin1pass**<br><br>Username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | Procedemos ahora a ingresar y configurar las lineas vty<br><br>Line vty 0 15<br>Login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | Configuramos ahora con el fin de que solo podamos en las líneas vty transportar por SSH<br><br>Transport input ssh |
| Cifrar las contraseñas de texto no cifrado | Debemos encriptar las contraseñas, caso contrario estas están en texto plano, para evitar esto debemos aplicar:<br><br>Service password-encryption |
| Configurar un MOTD Banner | Se configure el mensaje con el fin de evitar accesos no autorizados.<br><br>Banner motd % User Access Verification% |
| Generar una clave de cifrado RSA | En modo de configuración se coloca el comando para generar una clave de cifrado RSA así:<br><br>**Módulo de 1024 bits**<br><br>Crypto key generate rsa mosulus 10242 |

| Tarea | Especificación de Comandos |
|---|---|
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3<br>Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2**<br>Establecer la dirección IPv6 de capa 3<br>Int vlan 4<br>Ip address 10.19.8.98 255.255.255.248<br>Ipv6 address 2001:db8:acad:c::98/64<br>Ipv6 address fe80::98 link-local<br>Description MANAGEMENT<br>No shutdown |
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4<br><br>Ip Default-gateway 10.19.8.97 |

**Figura 7 – Configuración Básica de un Switch**

Evidencia del nombre del router, nombre de dominio configuradas en los pasos indicados en la tabla 7




Fuente: autor.

Paso 4: Continuamos nuestro proceso de configuración, esta vez con el S2, el proceso es muy similar ya que los parámetros que estamos configurando son los básicos, entonces, desactivamos la búsqueda de DNS de este, configuramos un nombre con el fin de identificarlo. Configuramos el respectivo dominio, configuramos todo lo relacionado con las contraseñas y las encriptamos de una vez, configuramos las líneas VTY y configuramos sus contraseñas, agregamos el mensaje BANNER MOTD que es el que aparece cada vez que queremos ingresar al dispositivo configuramos las VLAN y el Gateway predeterminado.

**Tabla 8 - Configuración básica S2 – configuración de nombre, dominio, contraseñas.**

| Tarea | Especificación de comandos |
|---|---|
| Desactivar la búsqueda DNS. | Se ingresa a modo privilegiado, luego se ingresa a modo de configuración y en seguida se coloca el comando para desactivar la búsqueda DNS así:<br><br>No ip domain lookup |
| Nombre del switch | En modo de configuración se coloca el comando para asignarle el nombre al Switch así:<br><br>**S1 o S2, según proceda**<br><br>Hostname S2 |
| Nombre de dominio | En modo de configuración se coloca el comando para asignarle el nombre de dominio así:<br><br>**ccna-lab.com**<br><br>ip domain name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | En modo de configuración se coloca el comando para asignar la contraseña para el modo EXEC privilegiado<br><br>**Ciscoenpass**<br><br>Enable secret ciscoenpass |

| Tarea | Especificación de comandos |
|---|---|
| Contraseña de acceso a la consola | En modo de configuración se coloca el comando para asignar la contraseña de acceso a la consola así:<br><br>**Ciscoconpass**<br><br>Line console 0<br>Password ciscoconpass<br>Login |
| Crear un usuario administrativo en la base de datos local | En modo de configuración se coloca el comando para crear un usuario administrativo en la base de datos local con el Nombre:<br><br>Nombre de usuario: **admin**<br>Password: **admin1pass**<br><br>Username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | En modo de configuración se coloca el comando para configurar el inicio de sesión en las líneas VTY así:<br><br>Line vty 0 15<br>Login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | En modo de configuración se coloca el comando para configurar VTY solo para que acepte SSH así:<br><br>Transport input ssh |
| Cifrar las contraseñas de texto no cifrado | Service password-encryption |
| Configurar un MOTD Banner | Banner motd % User Access Verification % |
| Generar una clave de cifrado RSA | **Módulo de 1024 bits**<br>Crypto key generate rsa modulus 1024 -- no soportado<br>Crypto key generate rsa 1024 |

| Tarea | Especificación de comandos |
|---|---|
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3<br>Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2**<br>Establecer la dirección IPv6 de capa 3<br>Int vlan 4<br>Ip address 10.19.8.99 255.255.255.248<br>Ipv6 address 2001:db8:acad:c::99/64<br>Ipv6 address fe80::99 link-local<br>Description MANAGEMENT<br>No shutdown |
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4<br>Ip Default-gateway 10.19.8.97 |

Paso 5: Continuamos la configuración de los SWITCH – S1 esta vez vamos a crear las VLAN y asignarle los nombres correspondientes, configuramos cada una de ellas asignando las respectivas direcciones IP y asignamos las interfaces que van a ser parte de la misma. Configuramos 802.1Q el cual va a ser el encargado del enrutamiento, la encapsulación y por consiguiente del intercambio de paquetes y de mensaje dentro de las subinterfaces, configuraremos los enlaces troncales que serán los caminos por los cuales estos paquetes se van a mover de manera fácil. Se configura las interfaces en modo acceso.

**Tabla 9 - VLAN TRUNKING en el S1.**

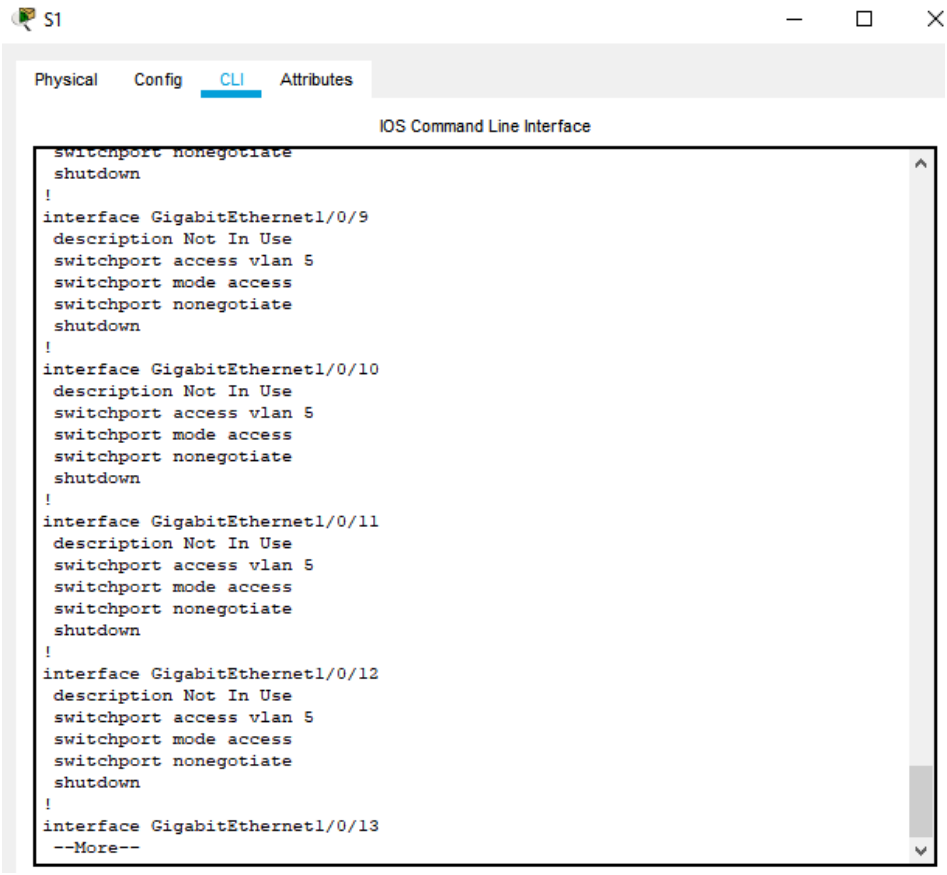
| Tarea | Especificación de comandos |
|---|---|
| Crear VLAN | Procedemos a crear nuestras VLAN, debemos antes que nada crearlas y luego nombrarlas.<br>Vlan 2<br>Name bikes<br>Vlan 3<br>Name trikes<br>Vlan 4<br>Name management<br>Vlan 5<br>Name parking<br>Vlan 6<br>Name native |

| Tarea | Especificación de comandos |
|---|---|
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | En modo de configuración se coloca el comando para troncos 802.1Q que utilicen la Vlan nativa así:<br><br>Interfaces F0/1, F0/2 y F0/5<br>Interfaces G1/0/1, G1/0/2 y G1/0/5<br><br>Debemos ingresar a la interfaz correcta.<br><br>Interface G1/0/5 **(ingresamos a la interfaz)**<br>Switchport trunk encapsulation dot1q<br>Switchport mode trunk **(configuramos como troncal)**<br>Switchport trunk native vlan 6 **(damos acceso a la vlan 6)**<br>Inteface range G1/0/1-2<br>Shutdown<br>Switchport trunk encapsulation dot1q<br>Switchport mode trunk<br>Switchport trunk native vlan 6 |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | En modo configuración se usa el protocolo LACP para la negociación con el siguiente comando:<br><br>Usar el protocolo LACP para la negociación<br><br>Channel-group 1 mode active<br>Int port channel 1<br>Switchport trunk encapsulation dot1q<br>Switchport mode trunk **(la configuramos como troncal)**<br>Switchport trunk native vlan 6 **(damos acceso a la VLAN 6)** |

| Tarea | Especificación de comandos |
|---|---|
| Configurar el puerto de acceso de host para VLAN 2 | En modo de configuración iniciamos llamamos la int f0/6 para configurar el puerto de acceso de host para Vlan 2 se utiliza el siguiente comando:<br><br>Interface F0/6<br>Interface g1/0/6 **(ingresamos a la interfaz que nos interesa)**<br>Switchport mode access **(confiuramos como modo de acceso)**<br>Switchport access vlan 2 **(le damos acceso a la VLAN 2)** |
| Configurar la seguridad del puerto en los puertos de acceso | En modo de configuración de la interfaz se configura para que solo permitir 3 direcciones MAC con el siguiente comando:<br>Permitir 3 direcciones MAC<br>Switchport port-security máximum 3 |
| Proteja todas las interfaces no utilizadas | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br><br>Int range g1/0/3-4 **(empleamos el commando RANGE para configurar varias interfaces al mismo tiempo)**<br>Switchport mode Access<br>Switchport Access vlan 5 **(les damos acceso a las vlan 5)**<br>Description no esta en uso **(agregamos una descripción sencilla para conocer mas)**<br>Shutdown<br>Int range g1/0/7-24<br>Switchport mode Access<br>Switchport Access vlan 5<br>Description no esta en uso<br>Shutdown<br>Int range g1/1/1-4<br>Switchport mode Access<br>Switchport Access vlan 5<br>Description no esta en uso<br>Shutdown |

**Figura 8 – Verificamos la creación de las VLAN y la asignación de la misma.**

Verificamos en el CLI la creación de las VLAN conforme a los pasos indicados en la tabla 9.




Fuente Autor.

Paso 6: Continuamos la configuración de los SWITCH – S2 esta vez vamos a crear las VLAN y asignarle los nombres correspondientes, configuramos cada una de ellas asignando las respectivas direcciones IP y asignamos las interfaces que van a ser parte de la misma. Configuramos 802.1Q el cual va a ser el encargado del enrutamiento, la encapsulación y por consiguiente del intercambio de paquetes y de mensaje dentro de las subinterfaces. Además parametrizaremos los enlaces troncales que serán los caminos por los cuales estos paquetes se van a mover de manera fácil. Se configura las interfaces en modo acceso.

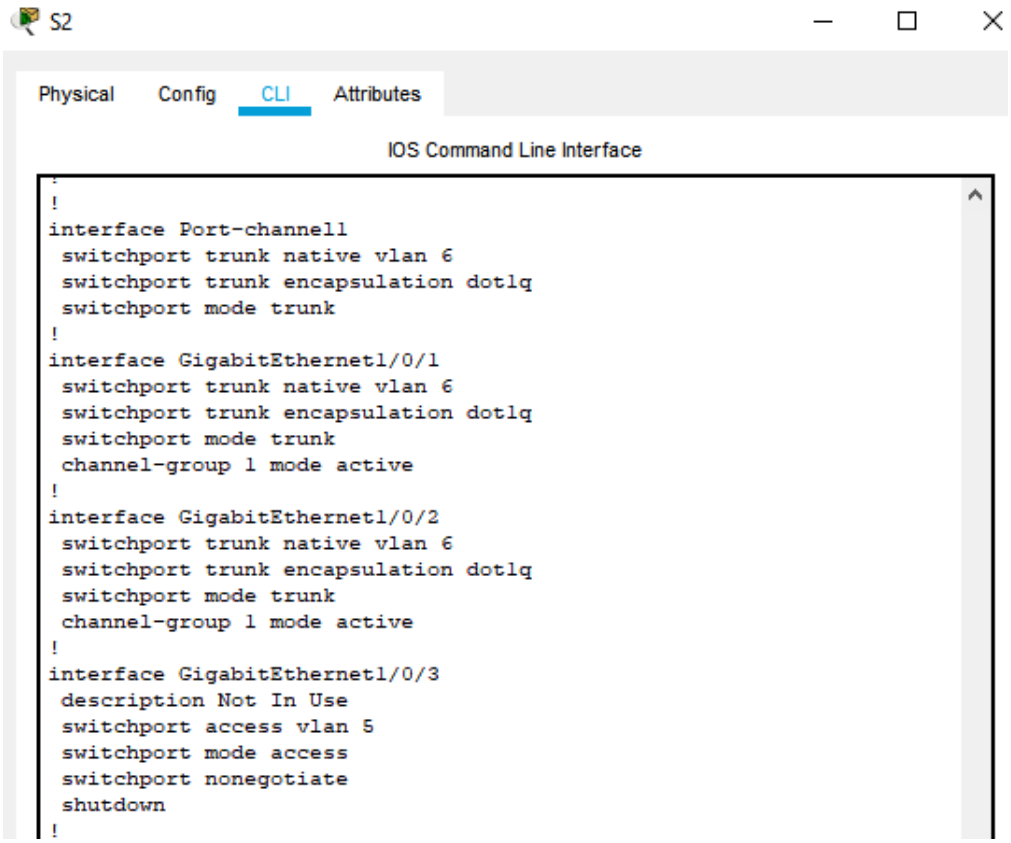
**Tabla 10 - VLAN TRUNKING en el S2.**

| Tarea | Especificación de comandos |
|---|---|
| Crear VLAN | Vlan 2<br>Name bikes<br>Vlan 3<br>Name trikes<br>Vlan 4<br>Name management<br>Vlan 5<br>Name parking<br>Vlan 6<br>Name native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Interfaces F0/1 y F0/2<br>Interfaces G1/0/1 y G1/0/2<br><br>Interfaces range G1/0/1-2 **(empleamos el commando RANGE para configurar varias interfaces al tiempo)**<br>Shutdown **(desactivamos)**<br>switchport trunk encapsulation dot1q<br>switchport mode trunk<br>switchport trunk native vlan 6 |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación<br><br>Channel-group 1 mode active<br>Int port channel 1<br>switchport trunk encapsulation dot1q **(activamos la encapsulación)**<br>switchport mode trunk **(configuramos como troncal)**<br>switchport trunk native vlan 6 **(acceso a la VLAN 6.)** |
| Configurar el puerto de acceso del host para la VLAN 3 | Interfaz F0/18<br><br>Int g0/1/18 **(ingresamos a la interfaz adecuada)**<br>Switchport mode Access **(config. modo acceso)**<br>Switchport Access vlan 3 **(acceso a la VLAN 3)** |

| Tarea | Especificación de comandos |
|---|---|
| Configure port-security en los access ports | **Reducimos la cantidad de direcciones MAC que se pueden conectar, en este caso 3 MAC,**<br><br>switchport port-security<br>switchport port-security maximum 3 |
| Asegure todas las interfaces no utilizadas. | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br><br>Int range g1/0/3-17 **(RANGE con el fin de configurar todas estas interfaces al tiempo)**<br>Switchport mode Access **(configuramos en modo acceso )**<br>Switchport Access vlan 5 **(les damos acceso a las VLAN 5)**<br>Description no esta en uso<br>Shutdown **(desactivamos)**<br><br>Int range g1/0/19-24<br>Switchport mode Access<br>Switchport Access vlan 5<br>Description no esta en uso<br>Shutdown<br><br>Int range g1/1/1-4<br>Switchport mode Access<br>Switchport Access vlan 5<br>Description no está en uso<br>Shutdown |
| Debemos activar las interfaces del etherchannel | S2:<br>G1/0/1-2<br>NO SHUTDOWN<br><br>S2:<br>G1/0/1-2<br>NO SHUTDOWN |

**Figura 9 – verificamos la creación de las VLAN y la asignación de la misma.**

Verificamos en el CLI la creación de las VLAN conforme a los pasos indicados en la tabla 10.




Fuente: autor.

Paso 5: Continuamos a configurar nuestro RUTER, comenzamos creando una ruta por defecto la cual apunta hacia INTERNET, si no tiene un camino para un mensaje todos serán enviados por esta ruta, configuramos ahora DHCP para las VLAN 2 Y 3 pero antes que nada debemos recordar que tenemos unas restricciones con relación a unas direcciones IP que no podemos utilizar de esta VLAN, para ello empleamos el comando EXCLUDED e indicamos cuales estarán por fuera del POOL DHCP

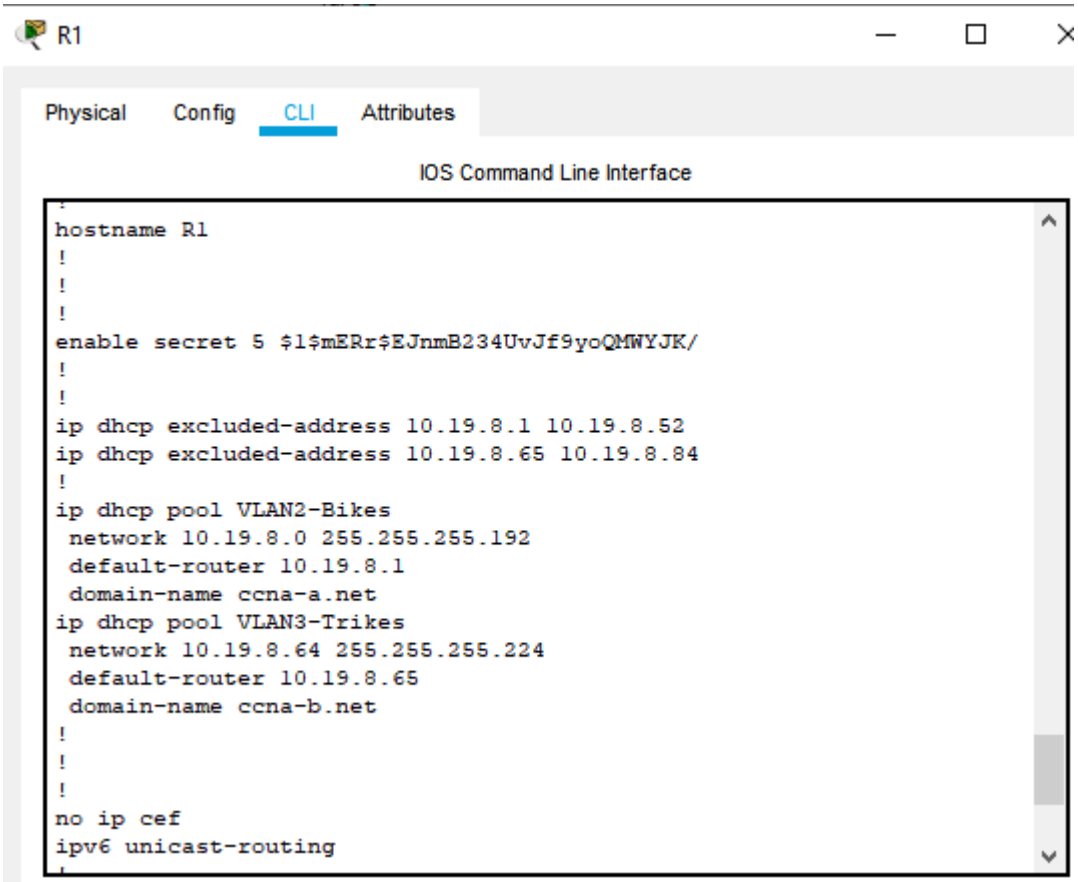
**Tabla 11 - Ruta por defecto en R1.**

| Tarea | Especificación de comandos |
|---|---|
| Configure Default Routing | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0<br>Ip route 0.0.0.0 0.0.0.0 loopback 0<br>Ipv6 route ::/0 loopback 0 |
| Configurar IPv4 DHCP para VLAN 2 | Cree un grupo DHCP para VLAN 2, compuesto por las **últimas 10 direcciones** de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada<br><br>10.19.8.0 /26<br>10.19.8.1<br>10.19.8.62<br>Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo.<br>10.19.8.1 - 10.19.8.52 estas son las que debemos restringir y solo trabajamos con las 10 que sobran.<br>Debemos entonces crear el POOL desde: 10.19.8.52 - 10.19.8.62<br>Ip dhcp excluded-address 10.19.8.1 10.19.8.52<br>Ip dhcp POOL VLAN2-BIKES<br>Network 10.19.8.0 255.255.255.192<br>Default-route 10.19.8.1<br>Domain-name ccna-b.net |

| Tarea | Especificación de comandos |
| --- | --- |
| Configurar DHCP IPv4 para VLAN 3 | Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada<br><br>TRIKES<br>10.19.8.64 /27<br><br>10.19.8.65<br>10.19.8.94<br><br>Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo.<br><br>10.19.8.65 - 10.19.8.84 estas son las que debemos restringir y solo trabajamos con las 10 que sobran.<br><br>Debemos entonces crear el POOL desde: 10.19.8.85 - 10.19.8.94<br><br>Ip dhcp excluded-address 10.19.8.65 10.19.8.84<br>Ip dhcp POOL VLAN3-TRIKES<br>Network 10.19.8.64 255.255.255.224<br>Default-route 10.19.8.65<br>Domain-name ccna-b.net |

**Figura 10 – DHCP y EXCLUDED en el router R1.**

Validamos en el CLI la configuración del DHCP para las VLAN creadas según pasos de tabla 11. Se observa que las restricciones si fueron creadas con relación a cada uno de los POOL siguiendo las indicaciones suministradas.

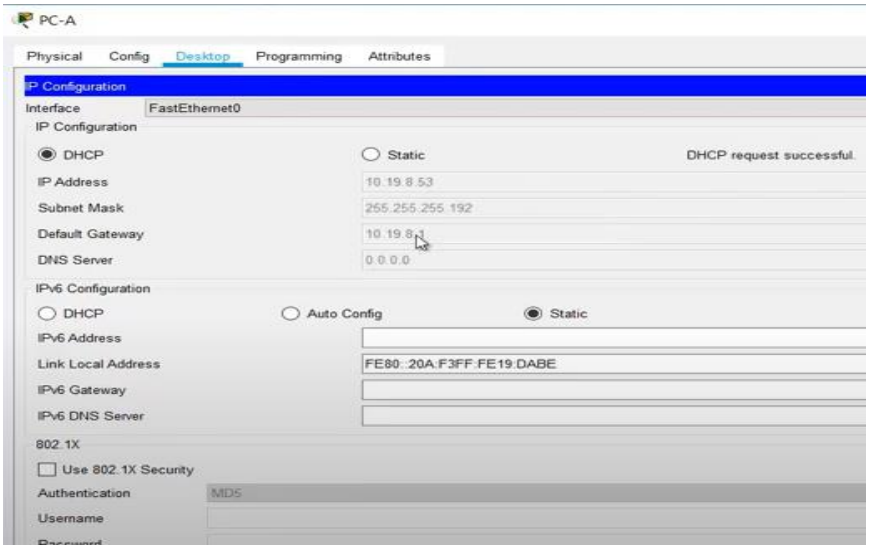



Fuente: autor.

Paso 6: Configurar los servidores host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

**Figura 11 - Verificación DHCP de PCA.**

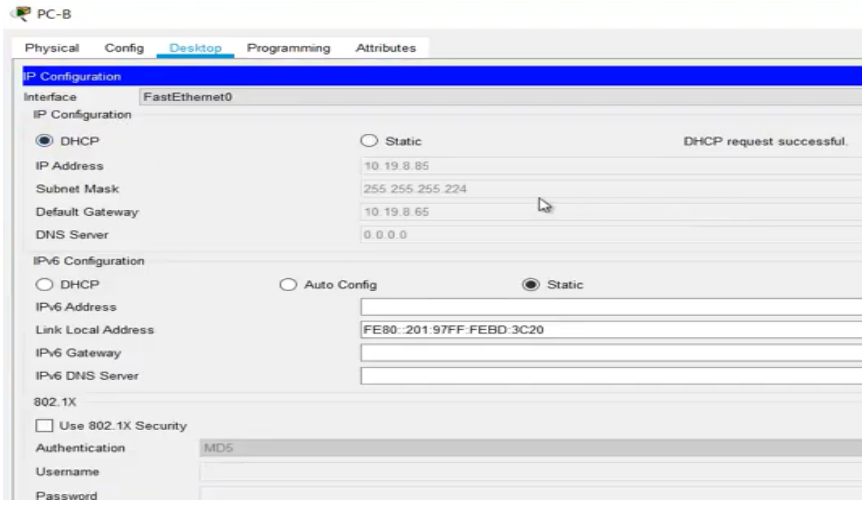
En la interfaz grafica del PC-A se configura que sea el DHCP quien asigne las direcciones IPv4




Fuente autor.

**Figura 12 - Verificación DHCP de PCB.**

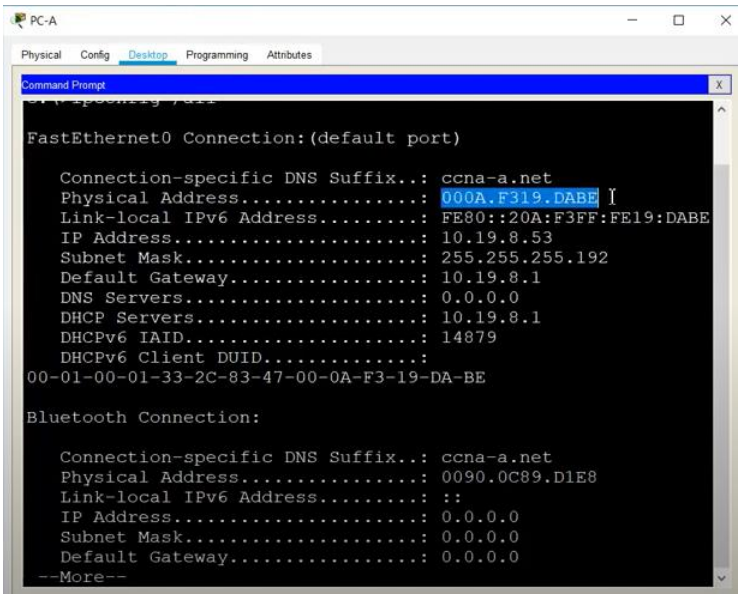
En la interfaz grafica del PC-A se configura que sea el DHCP quien asigne las direcciones IPv4




Fuente autor

**Figura 13 - Ipconfig PCA.**

En la consola de comandos con el ipconfig -all validamos que efectivamente los dispositivos están tomando la configuración adecuada




Fuente Autor.

**Tabla 12 Configuracion PC-A**

| PC-A Network Configuration | |
|---|---|
| Descripción | PC-A |
| Dirección física | 2001:DB8:ACAD:A::50 |
| Dirección IP | 10.19.8.53 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.19.8.1 |
| Gateway predeterminado IPv6 | FE80::1 |

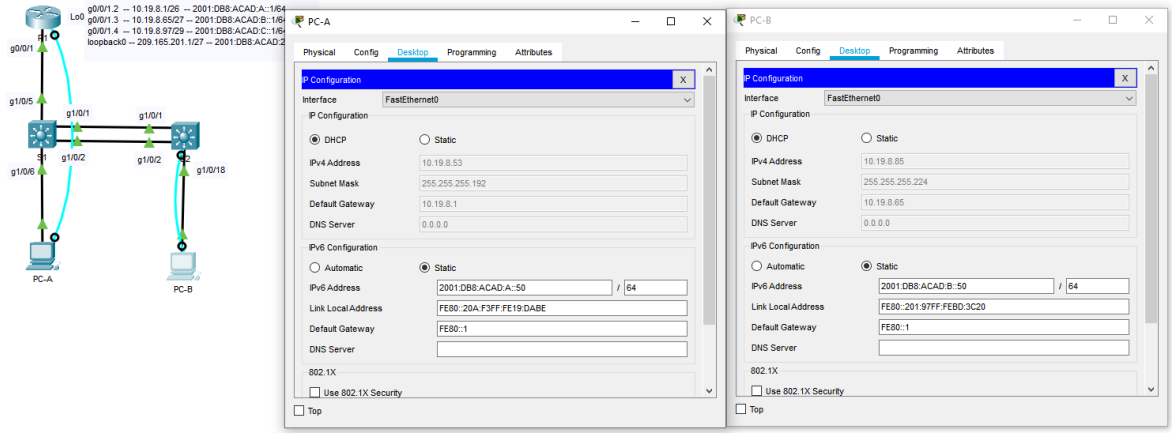
**Tabla 13 - Configuracion PC-B**

| Configuración de red de PC-B | |
|---|---|
| Descripción | PC-B |
| Dirección física | 2001:DB8:ACAD:B::50 |
| Dirección IP | 19.19.8.85 |

| Configuración de red de PC-B | |
|---|---|
| Máscara de subred | 255.255.255.224 |
| Gateway predeterminado | 10.19.8.65 |
| Gateway predeterminado IPv6 | FE80::1 |

**Figura 14 - Asignación DHCP PC-A y PC-B.**

Validamos en la interfaz grafica que se toman las configuraciones de red para IPv6 que se indican en las tablas 12 y 13




Fuente Autor.

Probar y verificar la conectividad de extremo a extremo Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

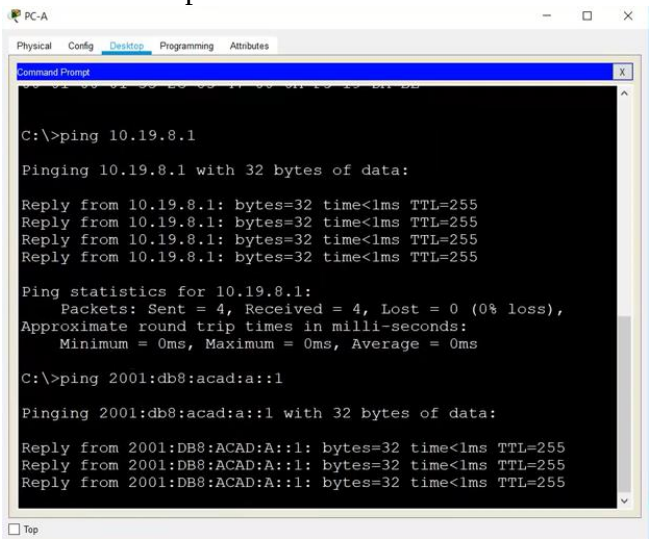
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

**Tabla 14 - prueba de conectividad desde PCA y PCB**

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1, G0/0/1.2 | Dirección | 10.19.8.1 | exitoso |
| PC-A | R1, G0/0/1.2 | IPv6 | 2001:db8:acad:a: :1 | exitoso |
| PC-A | R1, G0/0/1.3 | Dirección | 10.19.8.65 | exitoso |
| PC-A | R1, G0/0/1.3 | IPv6 | 2001:db8:acad:b: :1 | exitoso |
| PC-A | R1, G0/0/1.4 | Dirección | 10.19.8.97 | exitoso |
| PC-A | R1, G0/0/1.4 | IPv6 | 2001:db8:acad:c: :1 | exitoso |
| PC-A | S1, VLAN 4 | Dirección | 10.19.8.98 | exitoso |
| PC-A | S1, VLAN 4 | IPv6 | 2001:db8:acad:c: :98 | exitoso |
| PC-A | S2, VLAN 4 | Dirección | 10.19.8.99. | exitoso |
| PC-A | S2, VLAN 4 | IPv6 | 2001:db8:acad:c: :99 | exitoso |
| PC-A | PC-B | Dirección | IP address will vary. | exitoso |
| PC-A | PC-B | IPv6 | 2001:db8:acad:b: :50 | exitoso |
| PC-A | R1 Bucle 0 | Dirección | 209.165.201.1 | exitoso |
| PC-A | R1 Bucle 0 | IPv6 | 2001:db8:acad:209: :1 | exitoso |
| PC-B | R1 Bucle 0 | Dirección | 209.165.201.1 | exitoso |
| PC-B | R1 Bucle 0 | IPv6 | 2001:db8:acad:209: :1 | exitoso |
| PC-B | R1, G0/0/1.2 | Dirección | 10.19.8.1 | exitoso |
| PC-B | R1, G0/0/1.2 | IPv6 | 2001:db8:acad:a: :1 | exitoso |
| PC-B | R1, G0/0/1.3 | Dirección | 10.19.8.65 | exitoso |
| PC-B | R1, G0/0/1.3 | IPv6 | 2001:db8:acad:b: :1 | exitoso |
| PC-B | R1, G0/0/1.4 | Dirección | 10.19.8.97 | exitoso |
| PC-B | R1, G0/0/1.4 | IPv6 | 2001:db8:acad:c: :1 | exitoso |
| PC-B | S1, VLAN 4 | Dirección | 10.19.8.98 | exitoso |
| PC-B | S1, VLAN 4 | IPv6 | 2001:db8:acad:c: :98 | exitoso |
| PC-B | S2, VLAN 4 | Dirección | 10.19.8.99. | exitoso |
| PC-B | S2, VLAN 4 | IPv6 | 2001:db8:acad:c: :99 | exitoso |

**Figura 15 - PING IPV4 e IPV6.**

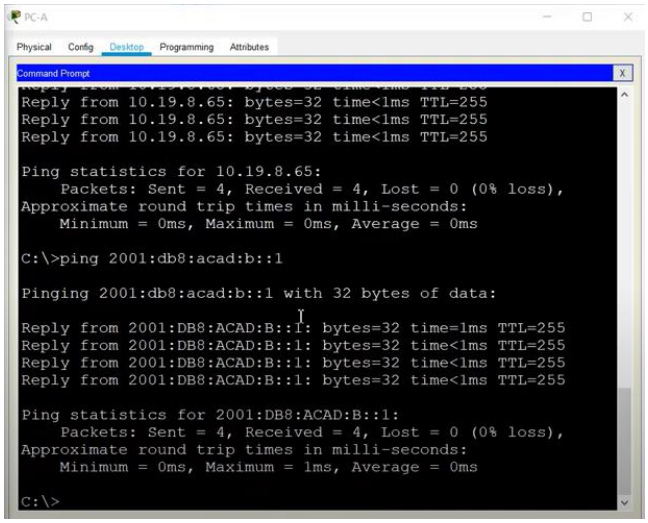
Ejemplo de un ping a la dirección ip 10.19.8.1 mostrando resultados exitosos.




Fuente autor.

**Figura 16 - PING IPV4 e IPV6 desde PCA.**

Ejemplo de un ping a la dirección ip 10.19.8.1 mostrando resultados exitosos.




Fuente autor.

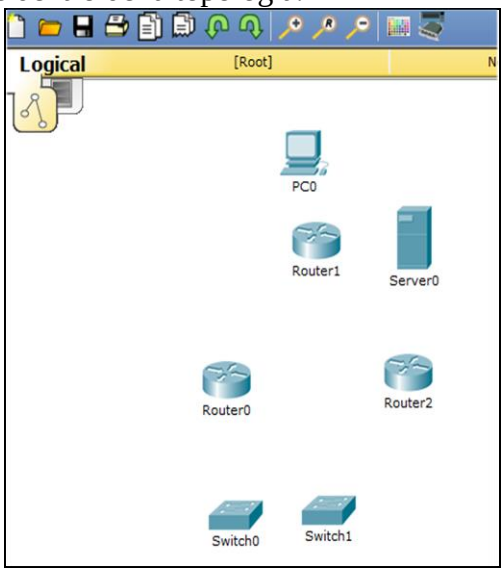
# 4. ESCENARIO 2

## 4.1 TOPOLOGIA

Procedemos a agregar al Packet Tracer los dispositivos necesarios para configurar la red solicitada.

**Figura 17 - Construcción ESCENARIO 2**

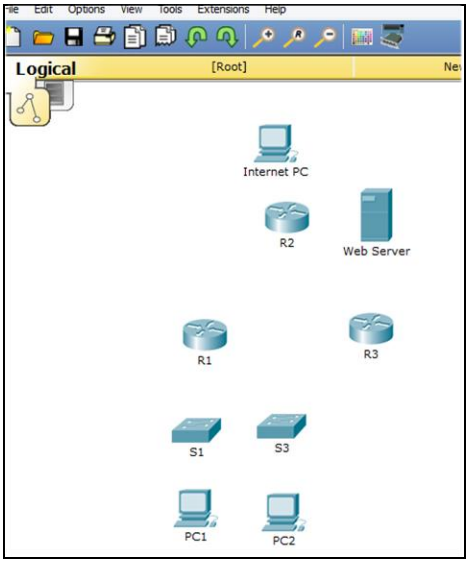
Asignación de dispositivos dentro de la topología.




Fuente Autor.

**Figura 18 - Construcción ESCENARIO 2**

Agregamos los dispositivos dentro de la interfaz del Packet Tracer




Fuente Autor.

Agregamos las interfaces físicas necesarias para cada dispositivo a través de la interfaz gráfica de la herramienta, se debe tomar en cuenta que el modelo de los dispositivos sea compatible con las interfaces de red necesarias para la conectividad.

**Figura 19 - Parte posterior del ROUTER.**

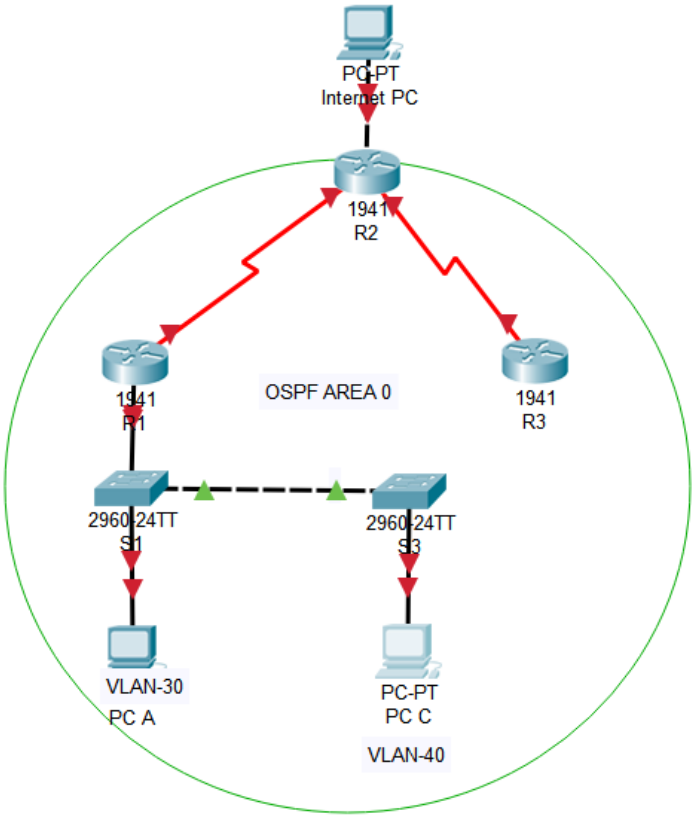

Fuente: cisco Packet tracer.

Agregamos las interfaces seriales al router Cisco 1941

**Figura 20 - Agregamos las interfaces al ROUTER.**


Fuente: cisco Packet tracer.

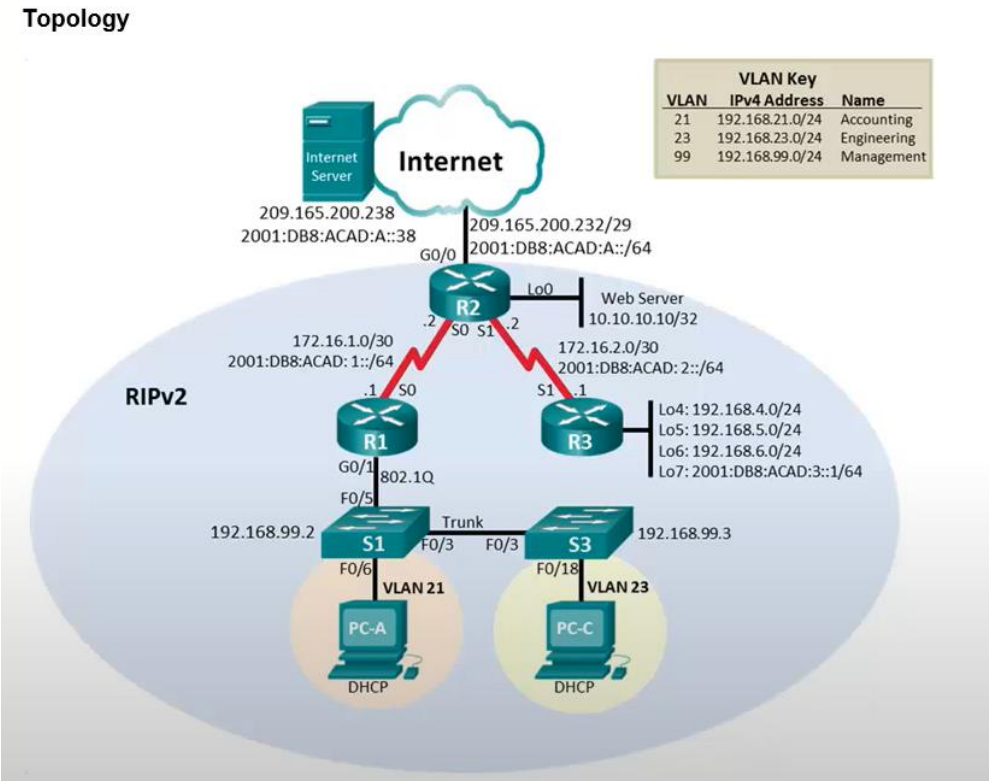
**Figura 21 - Topología final ESCENARIO 2 en Paket tracer.**




Fuente Autor.

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

**Figura 22 - Asignación de interfaces y rangos IP para cada subred.**




Fuente: Prueba de habilidades CCNA 2020, Cisco Academy.

## 4.2 INSTRUCCIONES

### Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches eliminando las configuraciones de inicio y volviendo a cargar los dispositivos, esto con el fin de evitar problemas de compatibilidad al momento de configurar la red.

**Tabla 15 – Inicializar los routers.**

| Tarea | Especificacion de comandos |
|---|---|
| Este proceso lo hacemos con el fin de evitar algún tipo de configuración anterior y que nos cause conflicto.<br>Todos los dispositivos les debemos aplicar el mismo.<br>Debemos hacer este proceso en todos los routers | Enable<br>Erase startup-config<br>Reload |
| Borramos la configuración de las VLAN de los switches<br>Borramos y reiniciamos<br>Este proceso lo debemos hacer en los 2 switches | Enable<br>Erase startup-config<br>Delete vlan.dat<br>Reload |
| Verificamos que no tenemos configurados VLANS | Show flash |

## Parte 2: Configurar los parámetros básicos de los dispositivos

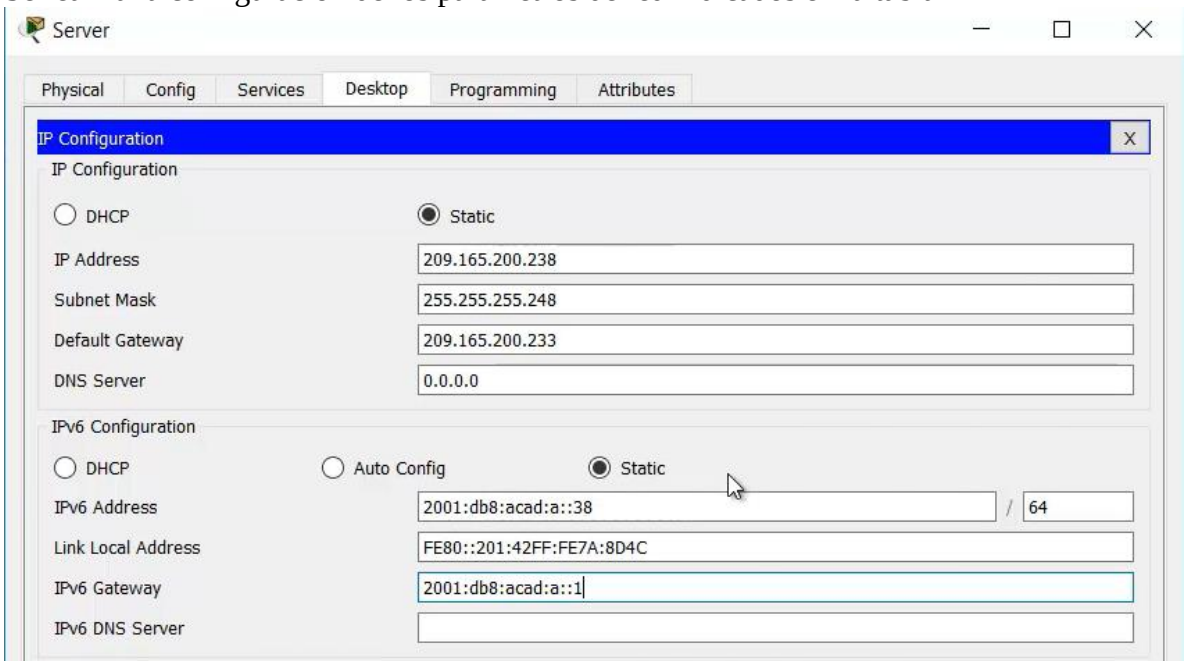
Paso 1: Configurar la computadora de Internet, para ello nos basaremos en la tabla 16 la cual nos indica la dirección ip, mascara de subred y Gateway tanto para IPv4 como IPv6. Esto lo configuraremos en la interfaz grafica del computador.

**Tabla 16 - 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 23 - configuración PC server.**

Se realiza la configuracion de los parámetros de red indicados en la tabla 1




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 desactivando el DNS y parametrizando nombres y contraseñas de acceso al dispositivo, posteriormente procedemos a configurar la dirección ip correspondiente y las rutas IP por defecto.

**Tabla 17 – Configuracion Basica R1**

| Tarea | Especificacion de comandos |
|---|---|
| Desactivamos DNS, configuramos los nombres y configuramos las contraseñas | Enable<br>Configure terminal<br>No ip domain lookup<br>Hostname R1<br>Enable secret class<br>Line console 0<br>Password cisco<br>Login<br>Line vty 0 15<br>Password cisco<br>Login<br>Service password-encryption |
| Configuramos el mensaje del dispositivo a ingresamos a la interfaz que nos corresponde y configuramos cada una de ellas, configuramos esta interfaz como clock rate. | Banner motd % User Access Verification  %<br>Int s 0/0/0<br>Descripción conexión con R2<br>Ip address 172.16.1.1 255.255.255.252<br>Ipv6 address 2001:db8:acad:1::1/64<br>No shutdown<br>Clock rate 128000 |
| Configurar las rutas por defecto IPV4 e IPV6 | Exit<br>Ip route 0.0.0.0 0.0.0.0 s0/0/0<br>Ipv6 route ::/0 s0/0/0 |

**Nota:** Todavía no configure G0/1.

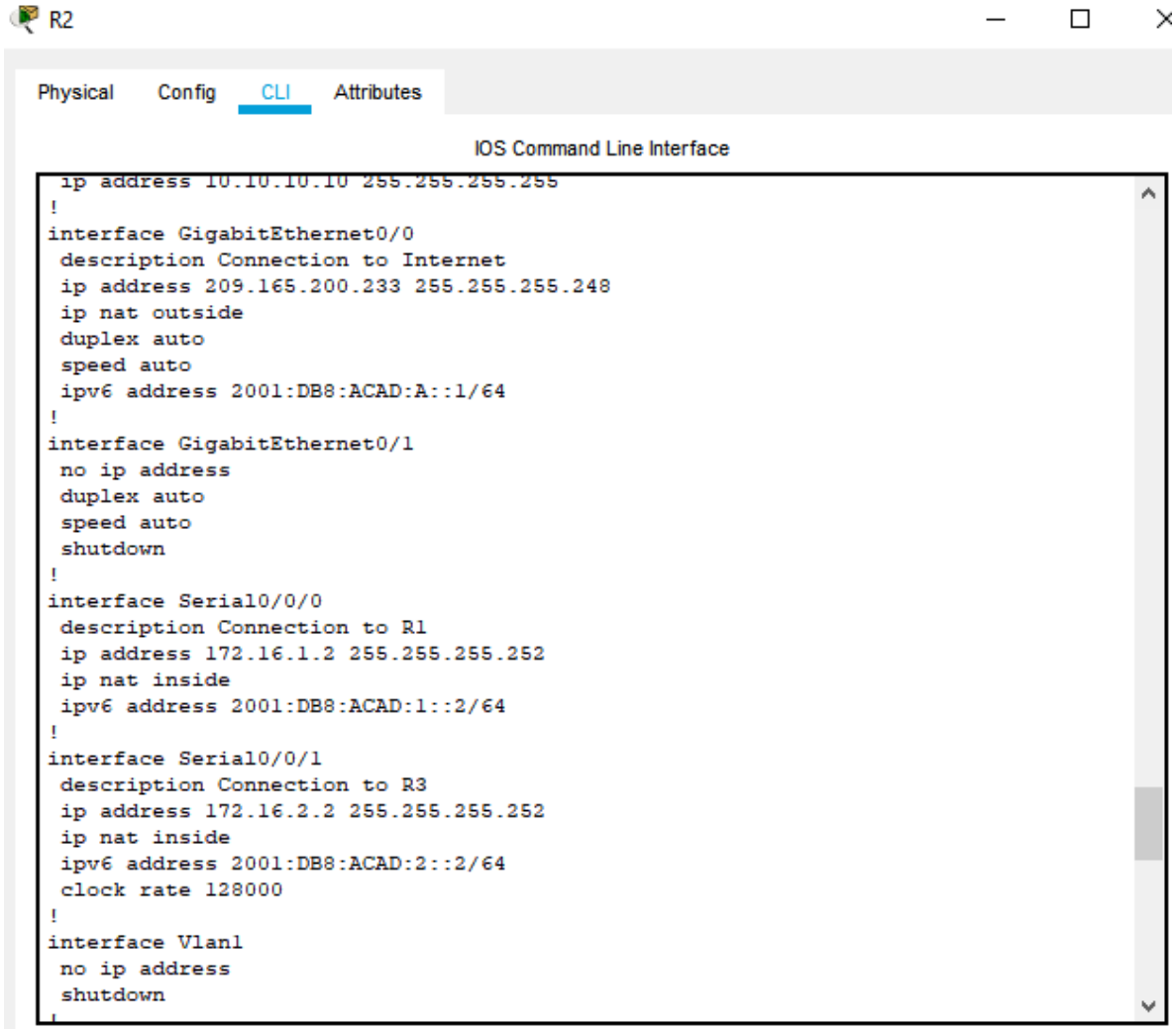
Paso 3: Configurar R2 desactivando el DNS y parametrizando nombres y contraseñas de acceso al dispositivo, posteriormente procedemos a configurar la dirección ip correspondiente y las rutas IP por defecto. Asimismo, debemos habilitar el servidor DHCP.

**Tabla 18 – Configuracion Basica R2**

| Tarea | Especificacion de comandos |
|---|---|
| Configuramos los datos más importantes del router, nombre, contraseñas, y aprovechamos para encriptar las mismas. | No ip domain-lookup<br>Hostname R2<br>Enable secret class<br>Line console 0<br>Password cisco<br>Login<br>Line vty 0 15<br>Password cisco<br>Login<br>Service password-encryption |
| | Habilitamos el servidor DHCP<br>Comando no soportado por PACKET TRACER. |
| Le configuramos a este router igualmente el mensaje de este y configuramos las interfaces Configuramos la interface serial | Banner motd % User Access Verification %<br><br>Interface serial 0/0/0<br>Description conexión con R1<br>Ip address 172.16.1.2 255.255.255.252<br>Ipv6 addres 2001:db8:acad:1::2/64<br>No shutdown |
| Procedemos a configurar la interface serial, agregamos una pequeña descripción, configuramos IPV4 como IPV6 y configuramos como clock rate. | Interface serial 0/0/1<br>Description conexión con R3<br>Ip address 172.16.2.2 255.255.255.252<br>Ipv6 addres 2001:db8:acad:2::2/64<br>Clock rate 128000<br>No shutdown |
| Procedemos ahora a configurar la interface g0/0 agregamos la descripción configuramos IPV4 e IPV6 y la activamos. | Interface g 0/0<br>Description conexión a INTERNET<br>Ip address 209.165.200.233 255.255.255.248<br>Ipv6 addres 2001:db8:acad:a::1/64<br>No shutdown |
| Configuramos ahora la interface loopback que nos va a permitir similar nuestro servidor y de una vez le asignamos una IP | Interface loopback 0<br>Description WEB SERVER<br>Ip address 10.10.10.10 255.255.255.255 |
| Creamos nuestra ruta por defecto tanto IP-V4 como IP – V6: | Ip route 0.0.0.0 0.0.0.0 g0/0<br>Ipv6 route ::/0 g0/0 |

**Figura 24 - configuración de interfaces ROUTER2.**

Se valida en el CLI que las configuraciones indicadas en la tabla 18 se aplicaron correctamente




Fuente: autor.

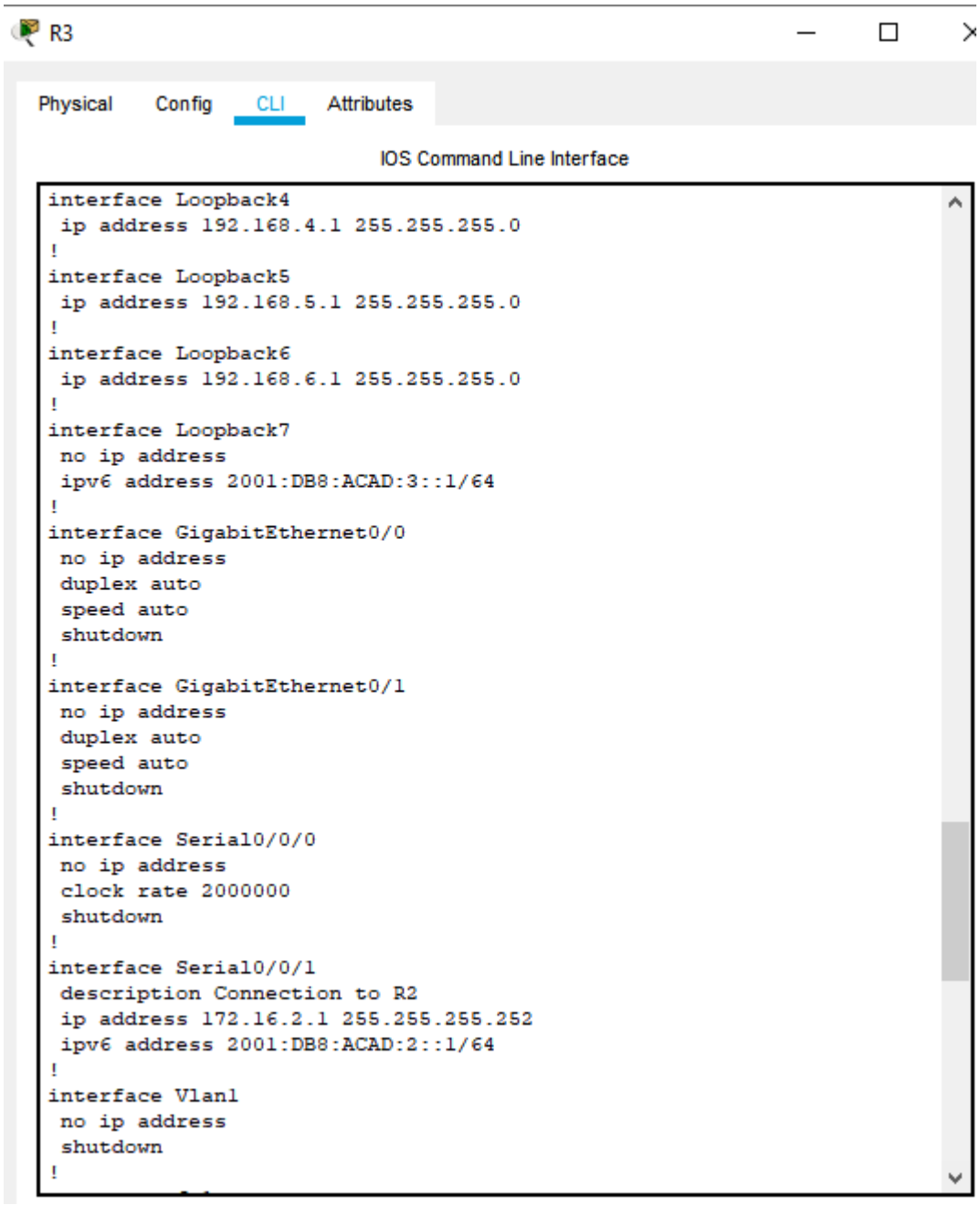
Paso 4: Configurar R3. Repetimos el proceso de las anteriores, tal como pueden seguir en la tabla a continuación

**Tabla 19 – Configuracion basica R3**

| Tarea | Especificacion de comandos |
|---|---|
| Configuramos los datos más importantes del router, nombre, contraseñas, y aprovechamos para encriptar las mismas. | No ip domain-lookp<br>Hostname R3<br>Enable secret class<br>Line console 0<br>Password cisco<br>Login<br>Line vty 0 15<br>Password cisco<br>Login<br>Service password-encryption |
| Le configuramos a este router igualmente el mensaje de este y configuramos las interfaces | Banner motd % User Access Verification % |
| Configuramos las interfaces | Interface s0/0/1<br>Description conexión con R2<br>Ip address 172.16.2.1 255.255.255.252<br>Ipv6 address 2001:db8:acad:2::1/64<br>No shutdown<br>Int loopback 4<br>Ip address 192.168.4.1 255.255.255.0 |
| Configuramos en este equipo cada una de las interfaces LOOPBACK | Int loopback 5<br>Ip address 192.168.5.1 255.255.255.0<br><br>Int loopback 6<br>Ip address 192.168.6.1 255.255.255.0<br><br>Int loopback 7<br>Ipv6 address 2001:db8:acad:3::1/64 |
| Creamos con el comando indicado las Rutas por defecto IPV4 como IPV6. | Ip route 0.0.0.0 0.0.0.0 s0/0/1<br>Ipv6 route ::/0 s0/0/1 |

**Figura 25 - configuración de interfaces ROUTER3.**

Se valida en el CLI que las configuraciones indicadas en la tabla 18 se aplicaron correctamente




Fuente: autor.

Paso 5: Configurar S1 procediendo a colocar los nombres y las contraseñas y a su vez un mensaje para los accesos que no están autorizados.

**Tabla 20 – Configuracion basica S1**

| Tarea | Especificacion |
|---|---|
| No ip domain lookup<br>Hostname S1<br>Enable secret class<br>Line console 0<br>Password cisco<br>Login<br>Line vty 0 15<br>Password cisco<br>Login<br>Service password-encryption | Comenzamos configurando los nombres, aplicamos la configuración de las contraseñas y encriptamos las contraseñas. |
| Banner moptd % acceso no autorizado% | Procedemos a configurar el mensaje |

Paso 6: Configurar el S3 de manera similar al S1

**Tabla 21 – Configuracion basica S3**

| Tarea | Especificacion |
|---|---|
| No ip domain lookup<br>Hostname S3<br>Enable secret class<br>Line console 0<br>Password cisco<br>Login<br>Line vty 0 15<br>Password cisco<br>Login<br>Service password-encryption | Comenzamos configurando los nombres, aplicamos la configuración de las contraseñas y encriptamos las contraseñas. |
| Banner moptd % acceso no autorizado% | Procedemos a configurar el mensaje: |

Paso 7: Verificar la conectividad de la red usando el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

**Tabla 22 - Verificación de conectividad desde R1 Y R2.**

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | Exitoso |
| R2 | R3, S0/0/1 | 172.16.2.1 | Exitoso |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | Exitoso |

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

En esta parte todos los PING deben ser satisfactorios, pues este se hace a la interfaz de un dispositivo conectado directamente.

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

Paso 1: Configurar en el S1 la base de datos de la VLAN asignándole una IP y una puerta de enlace. Luego se debe forzar el enlace troncal (Truncate) y no olvidar apagar los puertos que no se vayan a utilizar.

**Tabla 23 - VLAN y el routing entre VLAN S1**

| Tarea | Especificacion de Comandos |
|---|---|
| Proceso para configurar las VLANs | Vlan 21 **(creamos la VLAN)**<br>Name accounting **(asignamos un nombre a la misma)**<br>Vlan 23<br>Name engineering<br>Vlan 99<br>Name management |
| Asignar la IP a la VLAN MANAGEMENT | Interface vlan 99<br>Ip address 192.168.99.2 255.255.255.0<br>No shutdown |
| Asigne la puerta de enlace predeterminada | Ip default-gateway 192.168.99.1 |

| Tarea | Especificacion de Comandos |
|---|---|
| Forzar un enlace troncal | Int f 0/3 **(ingresamos a la interfaz adecuada)**<br>Switchport mode trunk **(configuramos modo troncal)**<br>Switchport trunk native vlan 1 **(acceso a la vlan 1)**<br><br>Int f 0/5<br>Switchport mode trunk<br>Switchport trunk native vlan 1<br><br>Int range f0/1-2, f0/4, f0/6-24, g0/1-2 **(desactivamos todas estas interfaces)**<br>Switchport mode access |
| Asignar f0/6 a la VLAN 21 | Int f 0/6<br>Switch port acces vlan 21 |
| Apague todos los puertos sin usar | Int range f0/1-2, f0/4, f0/7-24, g0/1-2<br>Shutdown |

Paso 2: Configurar el S3 de la misma manera que el S1 indicado anteriormente

**Tabla 24 - VLAN y el routing entre VLAN S3**

| Tarea | Especificacion de comandos |
|---|---|
| Crear la base de datos de la VLAN<br>Creamos la base de datos de la VLAN según la tabla de la topología | Vlan 21 **(creamos la VLAN)**<br>Name accounting **(asignamos un nombre a la VLAN)**<br>Vlan 23<br>Name engineering<br>Vlan 99<br>Name management |
| Asigne la IP a la VLAN MANAGEMENT | Interface vlan 99<br>Ip address 192.168.99.3 255.255.255.0<br>No shutdown |
| Asigne la puerta de enlace predeterminada | Ip default-gateway 192.168.99.1 |
| Forzar un enlace troncal | Int f 0/3<br>Switchport mode trunk<br>Switchport trunk native vlan 1 |
| Configurar todos los otros puertos como acceso | Int range f0/1-2, f0/4-24, g0/1-2<br>Switchport mode access |

| Tarea | Especificacion de Comandos |
|---|---|
| Asigne la f0/18 a la VLAN 23 | Int f0/18<br>Siwtchport Access vlan 23 |
| Apague todos los puertos sin usar | Int range f0/1-2, f0/4-17, f0/19-24, g0/1-2<br>Shutdown |

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

**Figura 26 – Tareas configuración R1**

Imagen de Cisco donde muestran las tareas de configuración para el R1

| Configuration Item or Task | Specification | Points |
|---|---|---|
| Configure 802.1Q subinterface .21 on G0/1 | Description Accounting LAN<br>Assign VLAN 21.<br>Assign the first available address to this interface. | (1 point) |
| Configure 802.1Q subinterface .23 on G0/1 | Description Engineering LAN<br>Assign VLAN 23.<br>Assign the first available address to this interface. | (1 point) |
| Configure 802.1Q subinterface .99 on G0/1 | Description Management LAN<br>Assign VLAN 99.<br>Assign the first available address to this interface. | (1 point) |
| Activate Interface G0/1 | | (1 point) |

Fuente: Cisco.

**Tabla 25 - configuracion vlans router 1.**

| Tarea | Especificacion de comandos |
|---|---|
| Se ingresa a la subinterface, se agrega la descripción. Luego se encapsula y asignamos la IP. | Int g0/1.21 **(ingresamos a la subinterface)**<br>Description VLAN 21 **(agregamos la descripción)**<br>Encapsulation dot1q 21 **(encapsulamos)**<br>Ip address 192.168.21.1 255.255.255.0 **(asiganamos la IP)**<br>Int g0/1.23<br>Description VLAN 23<br>Encapsulation dot1q 23<br>Ip address 192.168.23.1 255.255.255.0<br><br>Int g0/1.99<br>Description VLAN 99 |

| | |
|---|---|
| | Encapsulation dot1q 99<br>Ip address 192.168.99.1 255.255.255.0<br><br>Exit<br>Int g0/1<br>No shutdown |

Paso 4: Verificar la conectividad de la red usando el comando ping para probar la conectividad entre los switches y el R1**.**

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

**Tabla 26 - verificación conectividad desde S1Y S3**

| 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 |

**Figura 27 - PING de S1 hacia 192.168.99.1**

Ejecutamos un ping para valida lar la conexión desde el Switch 1 hacia la IP 192.168.99.1 a través de la VLAN 99.

```
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 = 0/1/7 ms

S1#
```

Fuente: Autor

**Figura 28 - PING de S3 hacia 192.168.99.1**

Ejecutamos un ping para valida lar la conexión desde el Switch 3 hacia la IP 192.168.99.1 a través de la VLAN 99

```
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 = 0/0/0 ms

S3#
```

Fuente: Autor

**Figura 29 - PING de S3 hacia 192.168.21.1**

Ejecutamos un ping para valida lar la conexión desde el Switch 3 hacia la IP 192.168.21.1 a través de la VLAN 21

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```

Fuente: Autor

## Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1. Este protocolo permite optimizar el rendimiento de la red ya que, mediante un algoritmo, calcula la ruta más corta entre dos puntos de la red que se desea conectar. En la tabla 27 se evidencian los pasos a seguir para su activación.

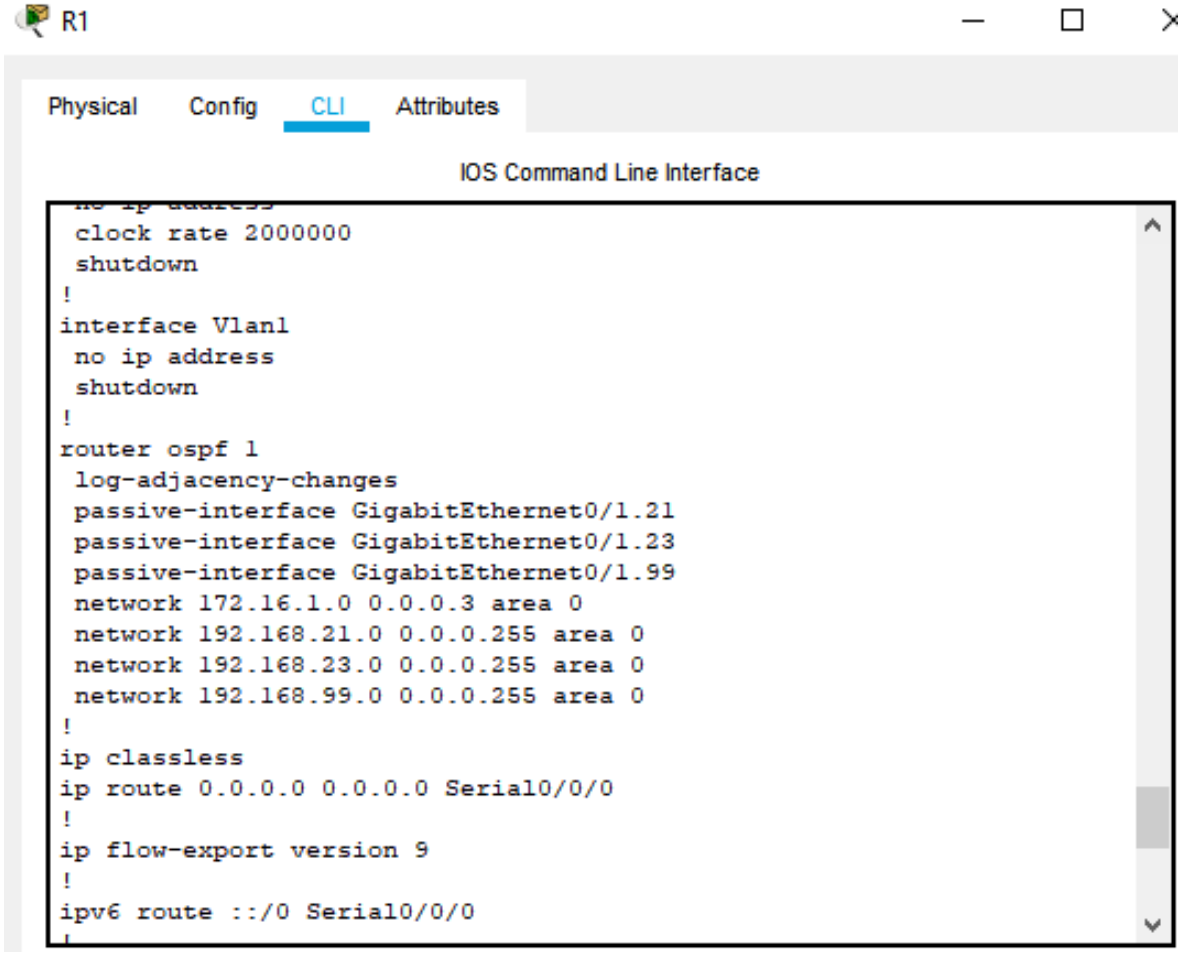
:

**Tabla 27 - Configuración OSPF R1.**

| Tarea | Especificación de comandos |
|---|---|
| Este es uno de los procesos más importantes, pues de este protocolo depende el enrutamiento de nuestra red, lo habilitamos | Configurar OSPF área 0<br>router ospf 1 |
| Debemos nombrar las redes que están conectados directamente al dispositivo que estamos configurando, nos podemos ayudar del comando SHOW IP ROUTE para conocer las redes que están conectada a nuestro equipo. | Anunciar las redes conectadas directamente<br>network 172.16.1.0 0.0.0.3 area 0<br>network 192.168.21.0 0.0.0.255 area 0<br>network 192.168.23.0 0.0.0.255 area 0<br>network 192.168.99.0 0.0.0.255 area 0 |
| Debemos declarar las interfaces hacia las cuales no queremos que lleguen actualizaciones como pasivas: | Establecer todas las interfaces LAN como pasivas<br>passive-interface GigabitEthernet0/1.21<br>passive-interface GigabitEthernet0/1.23<br>passive-interface GigabitEthernet0/1.99 |
| Desactivamos la sumarización automática con el fin de que todas las rutas sean publicadas de manera INDIVIDUAL | Desactive la sumarización automática<br>No auto-summary. |

**Figura 30 – OSPF configurado en R1.**

Validación en el CLI de los comandos ejecutados según la tabla 27 para configurar el protocolo OSPF en el Router 1




Fuente: autor.

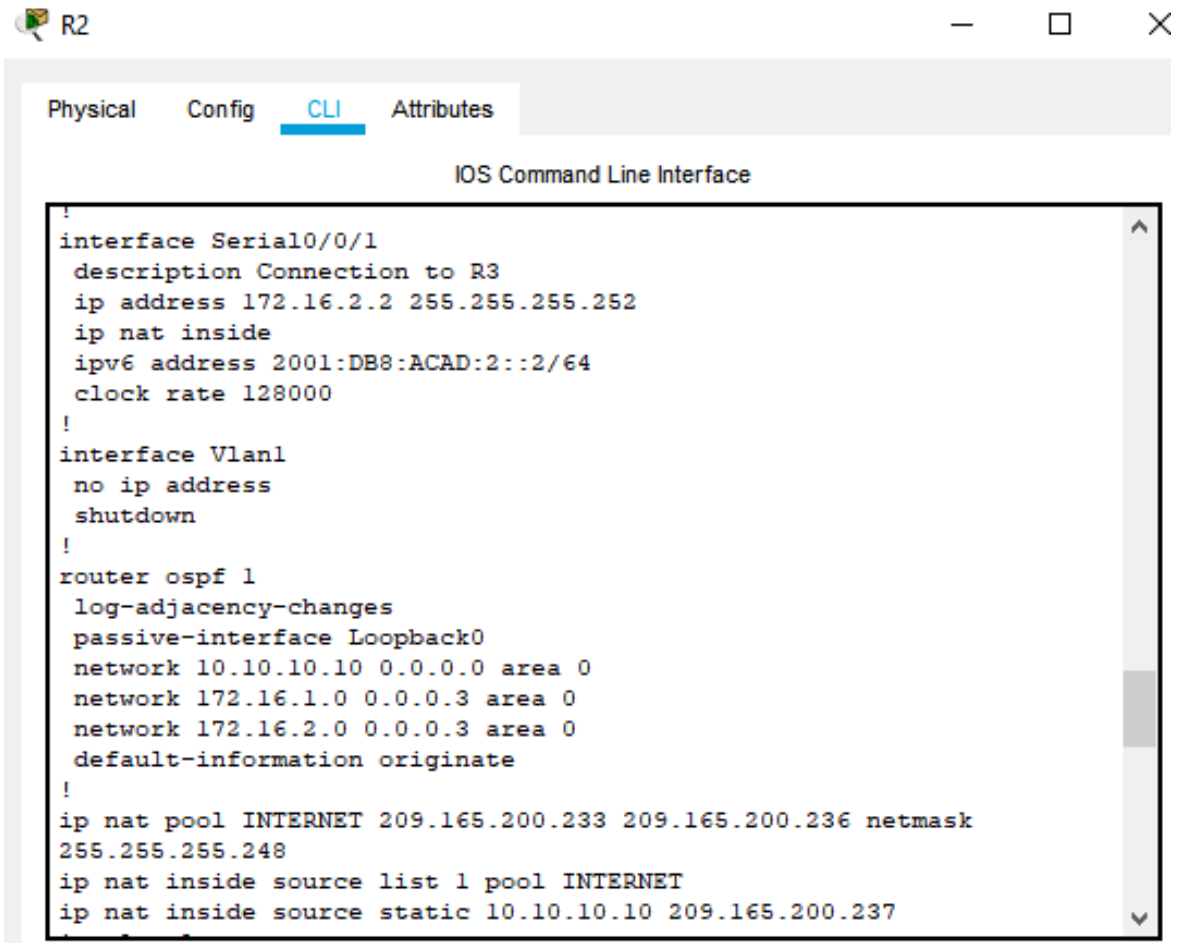
Paso 2: Configurar OSPF en el R2. Aquí repetimos el proceso realizado en el R2. Activando el protocolo en el router, indicar las redes que están conectadas y desactivar la sumarizacion automática.

**Tabla 28 - Configuracion OSPF R2.**

| Tarea | Especificación de comandos |
|---|---|
| Este es uno de los procesos más importantes, pues de este protocolo depende el enrutamiento de nuestra red, lo habilitamos. | Configurar OSPF área 0<br>router ospf 1. |
| Debemos nombrar las redes que están conectados directamente al dispositivo que estamos configurando, nos podemos ayudar del comando SHOW IP ROUTE para conocer las redes que están conectada a nuestro equipo.<br>**Nota:** Omitir la red G0/0. | Anunciar las redes conectadas directamente<br>network 10.10.10.10 0.0.0.0 area 0<br>network 172.16.1.0 0.0.0.3 area 0<br>network 172.16.2.0 0.0.0.3 area 0. |
| Debemos declarar las interfaces hacia las cuales no queremos que lleguen actualizaciones como pasivas | Establecer la interfaz LAN (loopback) como pasiva<br>passive-interface Loopback0. |
| Desactivamos la sumarización automática con el fin de que todas las rutas sean publicadas de manera INDIVIDUAL | Desactive la sumarización automática.<br>No auto summary. |

**Figura 31 – OSPF configurado en R2.**

Validación en el CLI de los comandos ejecutados según la tabla 27 para configurar el protocolo OSPF en el Router 1




Fuente: autor.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

**Tabla 29 - Configuración OSPF R3.**

| Tarea | Especificación de comandos |
|---|---|
| Este es uno de los procesos más importantes, pues de este protocolo depende el enrutamiento de nuestra red, lo habilitamos. | Configurar OSPF área 0<br>router ospf 1. |
| Debemos nombrar las redes que están conectados directamente al dispositivo que estamos configurando, nos podemos ayudar del comando SHOW IP ROUTE para conocer las redes que están conectada a nuestro equipo. | Anunciar redes IPv4 conectadas directamente<br>network 172.16.2.0 0.0.0.3 area 0<br>network 192.168.4.0 0.0.0.255 area 0<br>network 192.168.5.0 0.0.0.255 area 0<br>network 192.168.6.0 0.0.0.255 area 0. |
| Debemos declarar las interfaces hacia las cuales no queremos que lleguen actualizaciones como pasivas: | Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas<br>passive-interface Loopback4<br>passive-interface Loopback5<br>passive-interface Loopback6. |
| Desactivamos la sumarización automática con el fin de que todas las rutas sean publicadas de manera INDIVIDUAL | Desactive la sumarización automática.<br>No auto-summary. |

Paso 4: Verificar la información de OSPF

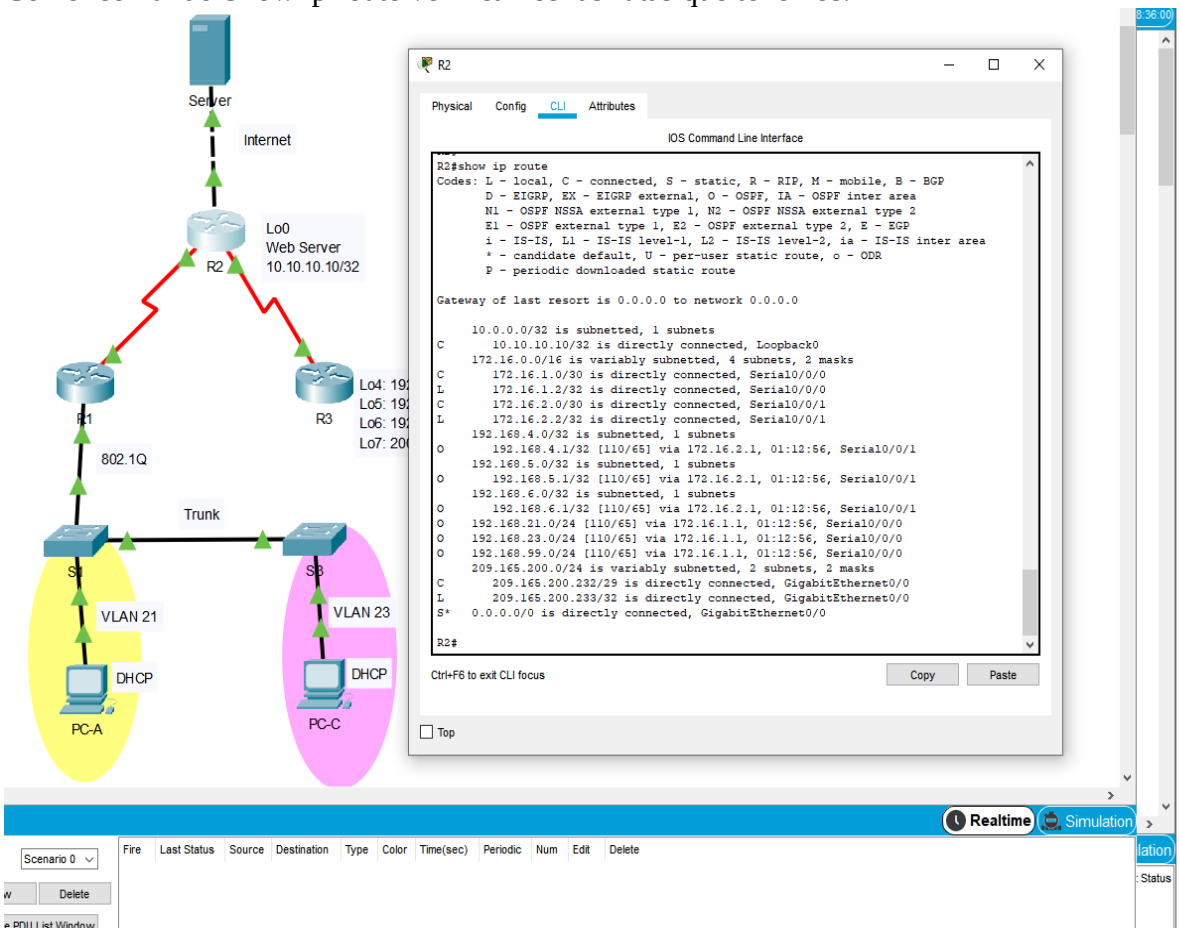
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

**Tabla 30 – Verificación 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 protocols<br>Commando. |

**Figura 32 – Show ip route**

Con el comando Show ip route verificamos las rutas que tenemos.




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:

**Tabla 31 - DHCP para las VLAN 21 y 23 EN R1.**

| Tarea | Especificacion de comandos |
|---|---|
| Reservas las primeras 20 direcciones de las VLAN 20 y 23 | Ip dhcp excluded-addess 192.168.21.1 192.168.21.20 **(indicamos las direcciones que vamos a excluir)**<br>Ip dhcp excluded-addess 192.168.23.1 192.168.23.20 **(indicamos las direcciones que vamos a excluir)** |
| Crear un POOL DHCP para la VLAN 21 | Ip dhcp pool **ACCT (cremamos el POOL y le asignamos un nombre)**<br>Network 192.168.21.0 255.255.255.0 **(le asignamos el rago ip)**<br>Default-router 192.168.21.1 **(indicamos el Puerto por defecto)**<br>Dns-server 10.10.10.10 **(indicamos la IP del DNS)**<br>Domain-name ccna-sa.com - comando no soportado |
| Crear un POOL DHCP para la VLAN 23 | Ip dhcp pool **ENGNR**<br>Network 192.168.23.0 255.255.255.0<br>Default-router 192.168.23.1<br>Dns-server 10.10.10.10<br>Domain-name ccna-sa.com - comando no soportado |

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

La configuración del R2 incluye las siguientes tareas:

**Tabla 32 - configuración NAT estática y dinámica en el R2**

| Tarea | Especificacion de comandos |
|---|---|
| Crear una base de datos LOCAL con una cuenta de usuario | Configure terminal<br>Username webuser privilege 15 secret cisco12345 |
| Habilitar HTTP SERVER | Ip http server -- comando no soportado |
| Autenticación local | Ip http authentication local -- comando no soportado |

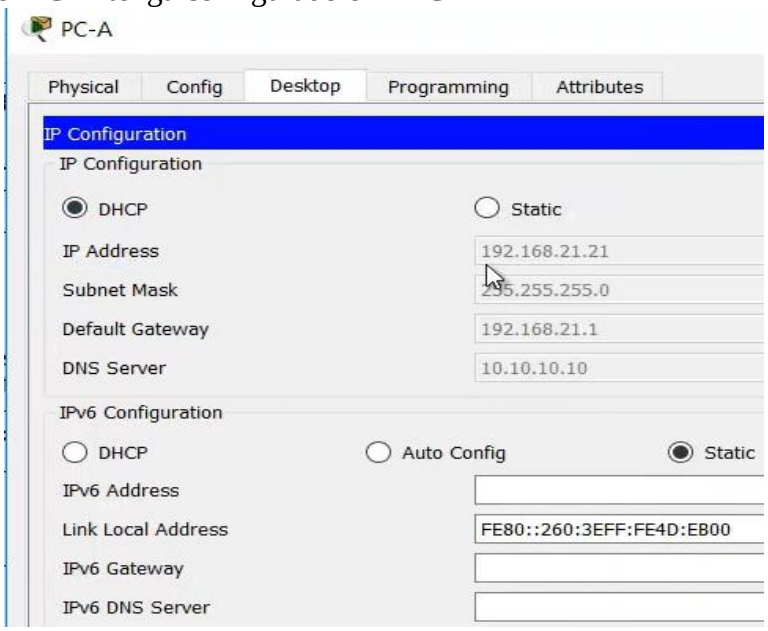
| | |
|---|---|
| Crear una NAT estadística para el servidor web. | Ip nate inside source static 10.10.10.10 209.165.200.23 |
| Debemos establecer las interfaces que entran y las que salen con el fin de que el dispositivo realice la traducción en el sentido correcto. | Entran:<br>Serial 0/0/0<br>Serial 0/0/1<br><br>Salen<br>G0/0<br><br>Int g0/0<br>Ip nat outside<br><br>Int s0/0/0<br>Ip nat inside<br>Int s0/0/1<br>Ip nat inside |
| Debemos ahora configurar la ACL NAT dinámica | Access-list 1<br>Access-list 1 permit 192.168.21.0 0.0.0.255<br>Access-list 1 permit 192.168.23.0 0.0.0.255<br>Access-list 1 permit 192.168.4.0 0.0.3.255<br>Ip NAT pool **INTERNET** 209.165.200.233 209.165.200.236 netmask 255.255.255.248<br>Ip nat inside source list 1 pool INTERNET |

Paso 3: Verificar el protocolo DHCP y la NAT estática.

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

**Figura 33 - PC-A verificación DHCP.**

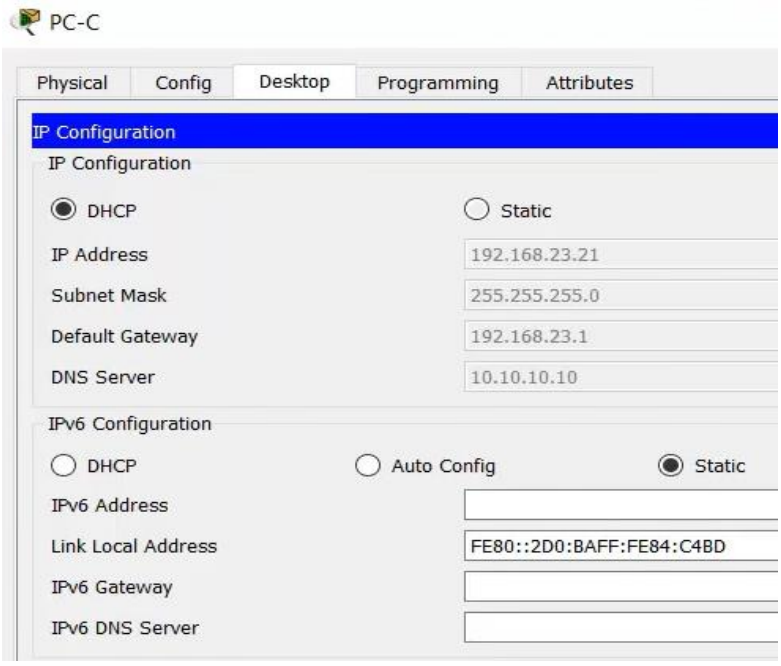
Se verifica que el PC-A tenga configurado el DHCP




Fuente autor.

**Figura 34 - PC-C verificación DHCP.**

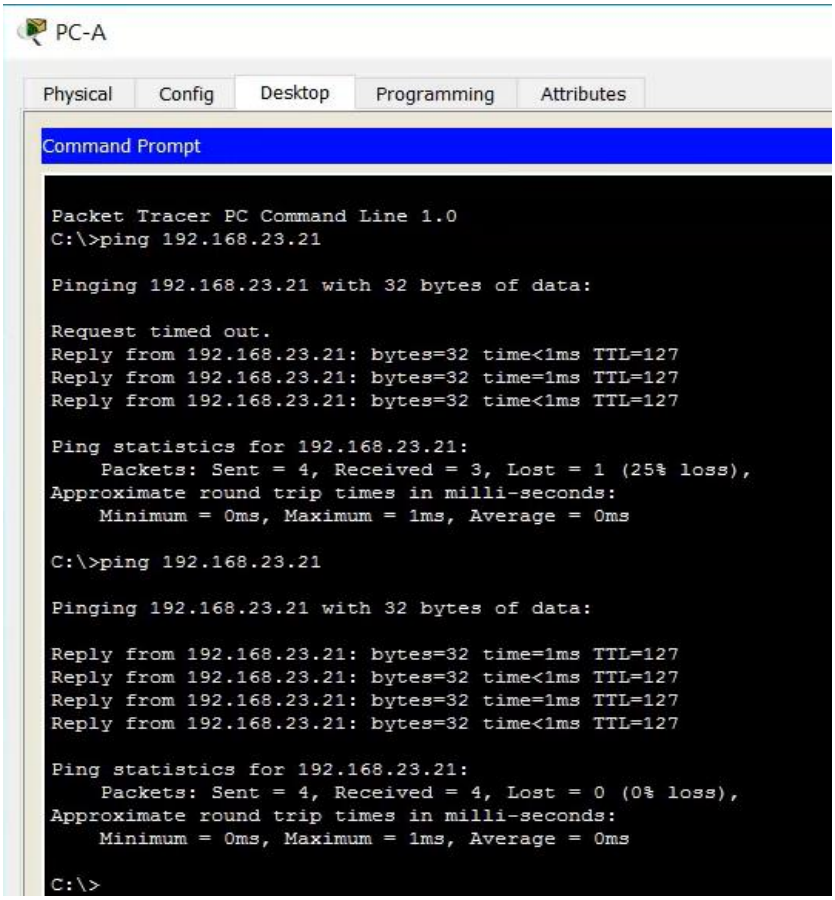
Se verifica que el PC-C tenga configurado el DHCP




Fuente Autor.

**Figura 35 – PING de PC-A hacia diferentes puntos de la red.**

Se valida la conectividad de PC – A hacia 192.168.23.21




Fuente Autor.

## Parte 6: Configurar NTP

La configuración de este comando debe hacerse en los ROUTERS, pero no es compatible en PACKET TRACER.

**Tabla 33 - configuracion NTP.**

| Tarea | Configuracion |
|---|---|
| Clock set 11:05:00 10 december 2017 | Configurar la fecha y hora en R2. |
| MASTER NTP | Configure R2 como MASTER 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

Demos restringir el acceso a VTY, para ello empleamos los siguientes comandos

**Tabla 34 - configuración VTY en R2.**

| Tarea | Configuracion |
|---|---|
| Ip Access-list standard ADMIN-MGT<br>Permit host 172.16.1.1<br>Exit | .<br>Restringir el acceso a VTY en R2. Solo R1 puede hacer TELNET a R2 |
| Line vty 0 15<br>Access-class ADMIN-MGT in<br>Transport input telnet | Debemos ahora aplicar esta ACL a las líneas VTY |

Procedemos en este punto a verificar que las ACL creadas estén funcionando correctamente:

**Figura 36 - verificación de TELNET desde R1,**

Se verifica con un Telnet que la configuración VTY en R2 hecha según la tabla 34 funcione correctamente

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!


User Access Verification

Password:
R2>exit

[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Fuente Autor.

**Figura 37 - verificación de TELNET desde R3.**

Se intenta hacer el mismo comando Telnet desde el R3 pero como no esta configurado, no es exitoso.

```
Unauthorized Access is Prohibited!

User Access Verification

Password:

R3>enable
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#
```

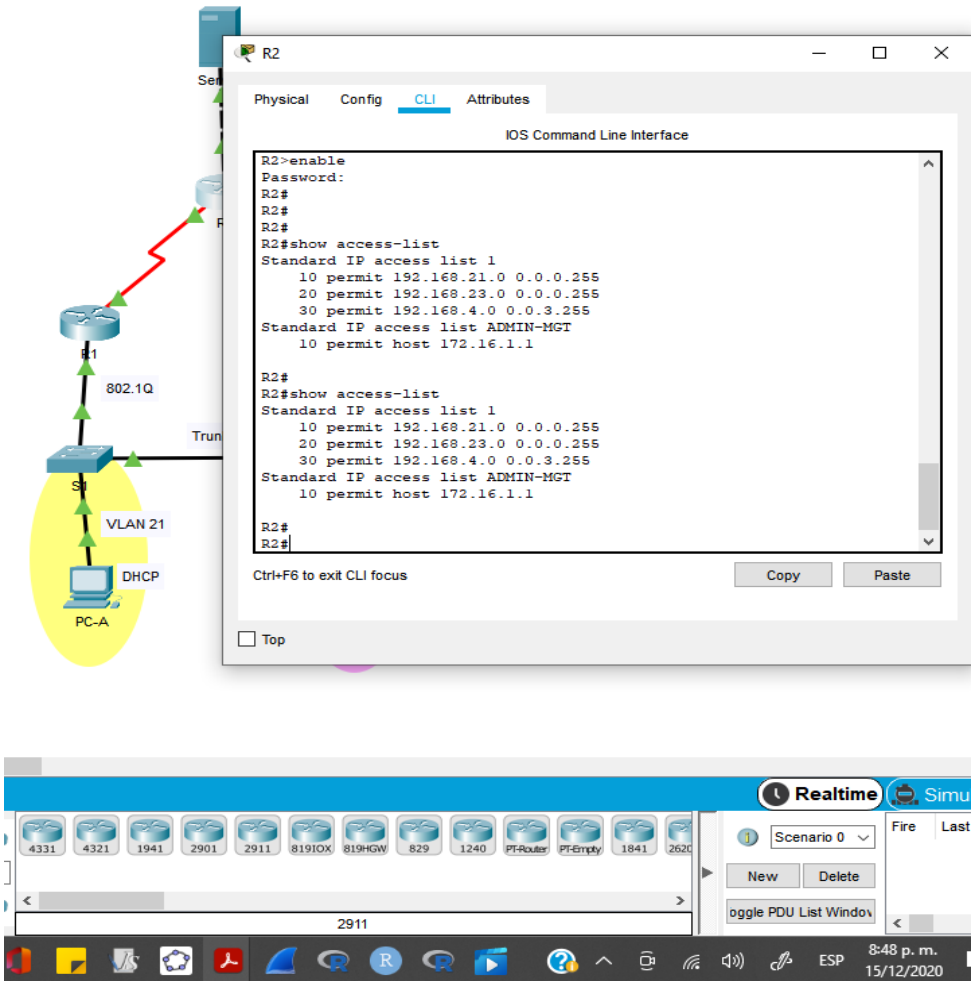
Fuente Autor.

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

**Tabla 35 - Comandos de verificación**

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | Show ip access-list |
| Restablecer los contadores de una lista de acceso | Clear 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 s0/0/0 |
| ¿Con qué comando se muestran las traducciones NAT? | Show ip nat translation<br>**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. |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | Clear ip nat translation * |

**Figura 38 – Verificamos las listas de control de acceso que tenemos configurados en este equipo.**
En esta imagen identificamos el uso del comando show access list donde se listan las direcciones IPs que han tenido acceso.




Fuente: autor.

**Figura 39 – clear ip access-list counters – no soportado**

Al ejecutar el comando clear ip access list se muestra en la consola CLI de la siguiente manera. Como se explico en la tabla 35 es usada para reestableces los contadores de acceso

```
R2#clear ip access-list counters
R2#clear ip
bgp Clear BGP connections
dhcp Delete items from the DHCP database
nat Clear NAT
ospf OSPF clear commands
route Delete route table entries

      R2#
```

Fuente: autor.

**Figura 40 – Show IP interface – verificar ACL.**

Ejemplo de como aplicamos el comando para mostrar el ACL que esta aplicando actualmente

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up
(connected) Internet address is 209.165.200.233/29
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not
set Inbound access list is
not set Proxy ARP is
enabled
Security level is default
Split horizon is enabled
```

Fuente: autor.

# 5. CONCLUSIÓN

A través del curso de profundización de redes Cisco se han tocado temas fundamentales a la hora de planificar, configurar y gestionar una red informática. Desde la configuración de los diferentes dispositivos físicos hasta la programación de puertos e interfaces virtuales, en cada paso del curso se han dejado claro los conceptos claves de redes.

Se han configurado redes de intranet, tal cual podemos ver en nuestras instituciones académicas o laborales, en donde a través de switchs, routers y servidores, es posible configurar una estructura de red fiable y sobre todo segura en donde a través de comandos específicos podemos definir los protocolos de comunicación con los cuales los usuarios podrán conectarse a ella.

Hemos profundizado bastante en lo que se refiere a configuración y puesta en marcha de diferentes protocolos de enrutamiento dentro de la misma red, OSPF, EIGRP, RIP V1, RIP V2. Los cuales son utilizados de manera estandarizada en redes WAN tales como las que nos proporcionan internet a nuestros hogares.

# 6. BIBLIOGRAFÍA Y WEBGRAFIA.


[1] CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

[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

[3] Palta Velasco, E. (10 de Julio de 2014). INTRODUCCIÓN A LA SEGURIDAD EN REDES. Recuperado el 10 de Marzo de 2015, de http://datateca.unad.edu.co/contenidos/233010/UNIDAD_No1_SEGURIDAD_EN_REDES.pdf

[4] Maestros del Web.(19 de Agosto del 2003).Sistemas de detección de intrusos. Recuperado el 17 de marzo del 2015, de http://www.maestrosdelweb.com

[5] W0LF_F4NG, 2020. Configuración Básica Ipv6 Router Cisco. [en línea] WF-Networking. Disponible en: https://www.w0lff4ng.org/configuracion-basica-ipv6-router-cisco/

[5] Willemvwyk, 2007. Err-Disabled On Fastethernet Port. [en linea] Community.cisco.com. Disponible en: https://community.cisco.com/t5/switching/err-disabled-on-fastethernet-port/td-p/716827

[6] Wikipedia, n.d. RSA. [en línea] Es.wikipedia.org. Disponible en: https://es.wikipedia.org/wiki/RSA

# ANEXOS

## ESCENARIO 1

Enlace de descarga de archivo de simulación del escenario 1 realizado en Packet Tracer alojado en Google drive: https://drive.google.com/file/d/1gNP8g774WvgeBSeHyb2-hvjdO25cvh9S/view?usp=sharing

## ESCENARIO 2

Enlace de descarga de archivo de simulación del escenario 2 realizado en Packet Tracer alojado en Google drive: https://drive.google.com/file/d/1hygoeUJiLpUCTbdL0xE6yGR2YdcEFdIV/view?usp=sharing

## FORMATO IEEE

Enlace de descarga del artículo científico "FORMATO IEEE - JHON JAIRO RAMIREZ" alojado en Google drive:

https://drive.google.com/file/d/1dSMFjp0GxlhkhO462cHJBNcVv5QEtvH-/view?usp=sharing

*JOHN JAIRO RAMIREZ GUEVARA*
*Universidad Nacional Abierta y a Distancia UNAD, jjramirezg@unadvirtual.edu.co*

**Resumen**

**En la presente actividad se va a desarrollar una solución para dos escenarios Corporativos en el cual aplicaremos la temática y nuestras destrezas relacionados con las redes y las telecomunicaciones, comenzaremos con toda la parte del diseño de la TOPOLOGIA con el fin de conocer la forma como los dispositivos va a estar conectados, sus interfaces y de esta manera conoce las subredes y la distribución de os equipos de entro de cada una de ellas, Por otra parte se continuará con la configuración de cada uno de los dispositivos que intervienen, PC, switches, routers, servidores, etc., todo ellos indicando desde la configuración más básica hasta aplicar los comandos que me permiten el intercambio de paquetes y la seguridad dentro de mi red.**

***Palabras clave:*** OSPF, RIP, Router, Switch, VLSM.

**Abstract:**

***In this activity, we will develop a solution for two Corporate scenarios in which we will apply the theme and our skills related to networks and telecommunications, we will begin with the entire design part of the TOPOLOGY in order to know how the devices will be connected, their interfaces and in this way you know the subnets and the distribution of the equipment inside each one of them.On the other hand, we will continue with the configuration of each of the devices involved, PCs, switches, routers, servers, etc., all of them indicating from the most basic configuration to applying the commands that allow me to exchange packets and security within my network.***

***Keywords*— OSPF, RIP, Router, Switch, VLSM.**

## I. Introducción

Como profesionales de las ramas de la ingeniería es de vital importancia poder practicar los conocimientos que hemos adquirido a lo largo de nuestra carrera y del Diplomado en el desarrollo de ESCENARIOS que nos exijan poner en práctica todas esas habilidades adquiridas. Es elemental para nuestra vida el hecho de poner en práctica cada uno de nuestros conocimientos, y más aún cuando este va encaminado a dar solución a inconvenientes que se presentan en nuestras sociedades.

La tecnología es mucho más asequible en nuestros días, por lo cual todos no importando muchas veces las clases sociales podemos estar inmersos dentro de su mundo, en nuestras vidas la tecnología ya es parte esencial para su correcto desarrollo
Ya no solo se tiene un ordenador para satisfacer todas las necesidades de cálculo de una organización, se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Son muchas las tecnologías que están avanzando a pasos agigantados, pero lo cierto es que debemos adaptarnos a esos cambios, y más como profesionales estar a la vanguardia de la misma y así poder brindar las mejores tecnologías a nuestra población.

A través de CISCO NETWORKING, en convenio con la Universidad Nacional Abierta y a Distancia, se pudo trabajar en dos módulos de redes LAN – WAN y CONFIGURACION DE ROUTERS, los cuales se fueron desarrollando de acuerdo al cronograma generado y de fácil acceso para todos. Desarrollaremos entonces 2 ESCENARIOS en los cuales configuraremos una serie de necesidades de las diferentes organizaciones.

## II. TIPOS DE ARTÍCULOS PUBLICABLES

El desarrollo del presente artículo es sobre INVESTIGACIÓN APLICADA, se pretende que a través de práctica todo el conocimiento adquirido se convierta en una destreza que podamos emplear para la solución de muchos problemas de este tipo.

## III. Parte Técnica del Artículo

La red que para mi caso se va a desarrollar es lo relacionado al ECENARIO 2, el diagrama de su topología es la que indico a continuación, en el mismo vamos a configurar una red pequeña la cual admita tanto IPV4 como IPV6 se configurará todo lo relacionado a la seguridad, el ruteo entrega las VLAN, OPSF, configuraremos protocolo de configuración de hosts dinámicos (DHCP). Todo esto con el fin de tener una red totalmente funcional. El diagrama de topología de la misa es el siguiente:

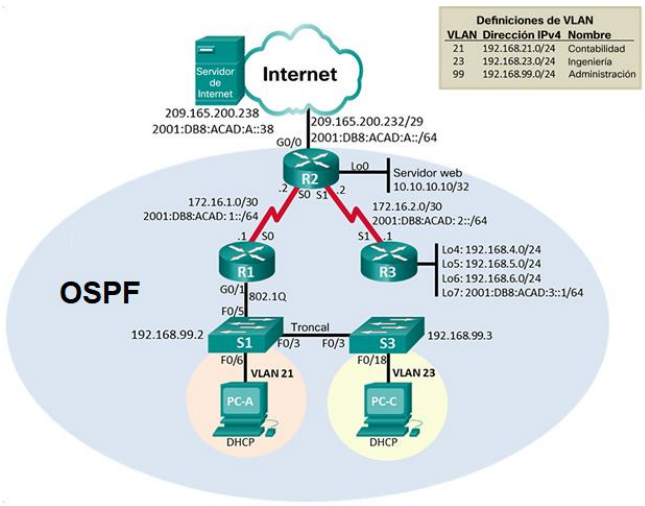



Figura 1 - TOPOLOGIA ESCENARIO 2.

INICIALIZAR DISPOSITIVOS:

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Recodemos que esta es una configuración básica la cual la podemos aplicar a todos los dispositivos de la red, llámese routers o switches.

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Enable<br>Erase startup-config<br>Reload |
| Volver a cargar todos los routers | Enable<br>Erase startup-config<br>Delete vlan.dat<br>Reload<br><br>Borramos y reiniciamos<br>Este proceso lo debemos hacer en los 2 switches |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | *Erase startup-config*<br>*Delete vlan.dat* |
| Volver a cargar ambos switches | *Reload* |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | *Show vlan brief*<br>*Show flash* |

**Tabla 1: reinicializar dispositivos.**

Ya que tenemos la topología de nuestra red bien clara, los dispositivos que intervienen y las interfaces que están conectadas, podemos proceder a realizar nuestra tabla de direccionamiento, esto con el fin de asignar a cada uno la correspondiente dirección IPV4 como también IPV6, esta asignación queda de la siguiente manera, no olvidemos que los rangos que se asigna para cada de estas subredes se indica dentro del mismo DIAGRAMA DE TOPOLOGÍA.

CONFIGURACIÓN DISPOSITIVOS:

Esta es otra parte sencilla que debemos hacer en todos los dispositivos, desde asignación de nombres, configuración de contraseñas, rutas por defecto, etc., el proceso se indica en uno de los dispositivos:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | No ip domain-lookup |
| Nombre del router | R2<br>Hostname R2. |
| Contraseña de exec privilegiado cifrada | Class<br>Enable secret class |
| Contraseña de acceso a la consola | Cisco<br>Line console 0<br>Password cisco<br>Login . |
| Contraseña de acceso Telnet | Cisco<br>Line vty 0 15<br>Password cisco<br>Login . |
| Cifrar las contraseñas de texto no cifrado | Service password-encryption. |
| Habilitar el servidor HTTP | Comando no soportado por PACKET TRACER. |
| Mensaje MOTD | Banner motd % Se prohíbe el acceso no autorizado. |
| Interfaz S0/0/0 | Interface serial 0/0/0<br>Description conexión con R1<br>Ip address 172.16.1.2 255.255.255.252<br>Ipv6 addres 2001:db8:acad:1::2/64<br>No shutdown |

| | |
|---|---|
| Interfaz S0/0/1 | Interface serial 0/0/1<br>Description conexión con R3<br>Ip address 172.16.2.2 255.255.255.252<br>Ipv6 addres 2001:db8:acad:2::2/64<br>Clock rate 128000<br>No shutdown |
| Interfaz G0/0 (simulación de Internet) | Interface g 0/0<br>conexión a Internet<br>Ip address 209.165.200.233 255.255.255.248<br>Ipv6 addres 2001:db8:acad:a::1/64<br>No shutdown |
| Interfaz loopback 0 (servidor web simulado) | Interface loopback 0<br>Description WEB SERVER<br>Ip address 10.10.10.10 255.255.255.255 |
| Ruta predeterminada | Ruta por defecto<br>Ip route 0.0.0.0 0.0.0.0 g0/0<br>Ipv6 route ::/0 g0/0 |

Tabla 2: Configuración básica Dispositivos.

Procedemos en este momento a configurar las interfaces VLAN, en los dispositivos que corresponden, y demás lo enlaces troncales.

| Tarea | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Int g0/1.21<br>Description VLAN 21<br>Encapsulation dot1q 21<br>Ip address 192.168.21.1 255.255.255.0. |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Int g0/1.23<br>Description VLAN 23<br>Encapsulation dot1q 23<br>Ip address 192.168.23.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Int g0/1.99<br>Description VLAN 99<br>Encapsulation dot1q 99<br>Ip address 192.168.99.1 255.255.255.0. |
| Activar la interfaz G0/1 | Exit<br>Int g0/1<br>No shutdown |

Tabla 3: Configuración de VLANS

Configuramos los protocolos de enrutaniento, para nuestro caso OSPF es el protocol que se va a encargar del intercambkio de mensajes en toda la red.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | router ospf 1 |
| Anunciar las redes conectadas directamente | network 172.16.1.0 0.0.0.3 area 0<br>network 192.168.21.0 0.0.0.255 area 0<br>network 192.168.23.0 0.0.0.255 area 0<br>network 192.168.99.0 0.0.0.255 area 0. |
| Establecer todas las interfaces LAN como pasivas | *passive-interface GigabitEthernet0/1.21*<br>*passive-interface GigabitEthernet0/1.23*<br>*passive-interface GigabitEthernet0/1.99* |
| Desactive la sumarización automática | No auto-summary. |

Tabla 4: Configuración de OSPF.

No olvidemos que este protocolo se debe configurar dentro de los ROUTERS.

Verifiquemos que nuestra red este funcionando, que los comandos ingresados sean los correctos y que estén bien aplicados:

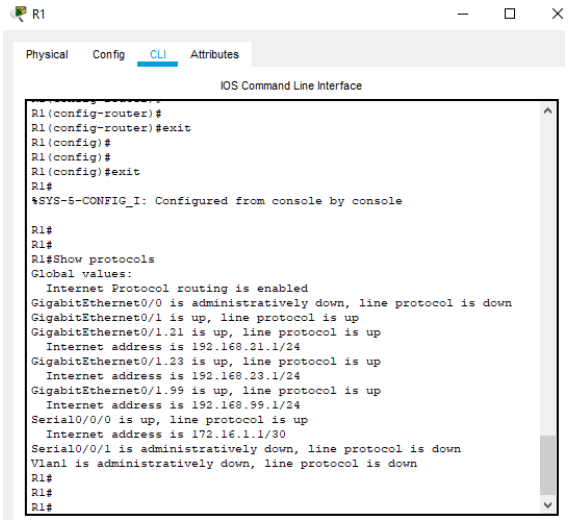



**Figura 11 - show protocols R1.**

| | |
|---|---|
| ¿Qué comando muestra solo las rutas OSPF? | *Show ip route ospf* |

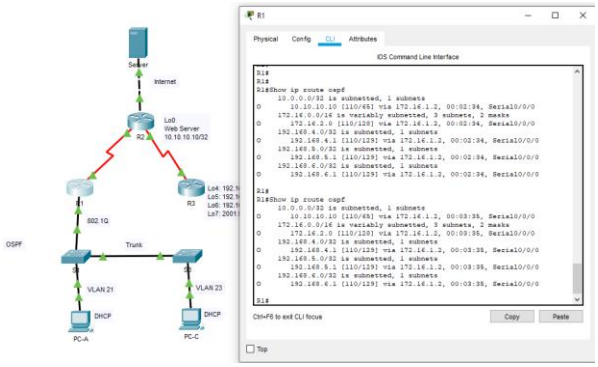



Figura 2- show ip route ospf en R1

| | |
|---|---|
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | *show running-config \| section ospf* |

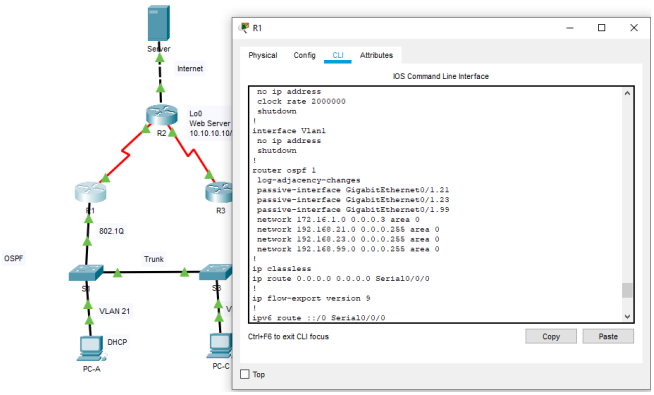



Figura 3- show ip route ospf en R1

**IMPLEMENTACION DE DHCP Y NAT.**

Procedemos a la descripción del último paso que debeos emplear en nuestra red, para ello debemos cumplir igualmente con una serie de restricciones, las mismas se indican a continuación:

| **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<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado<br><br>ip dhcp pool ACCT<br>network 192.168.21.0 255.255.255.0<br>default-router 192.168.21.1<br>dns-server 10.10.10.10. |

| | |
|---|---|
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado<br><br>ip dhcp pool ENGNR<br>network 192.168.23.0 255.255.255.0<br>default-router 192.168.23.1<br>dns-server 10.10.10.10<br>. |

Tabla 5: Configuración de DHCP Y NAT.

Verificamos que la configuración hecha sea correcta:

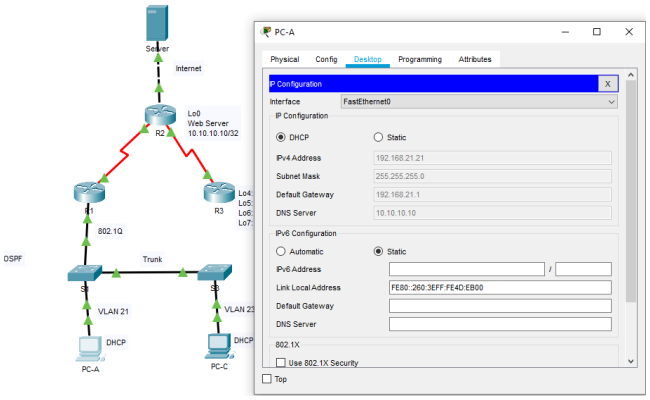


**Figura 4 - verificación DHCP en PC-A.**

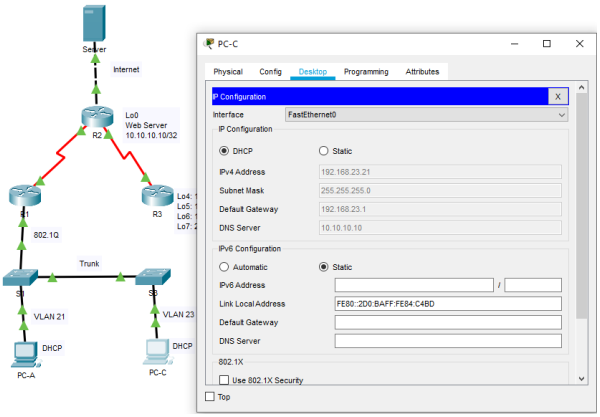


**Figura 5 - verificación DHCP en PC-C.**

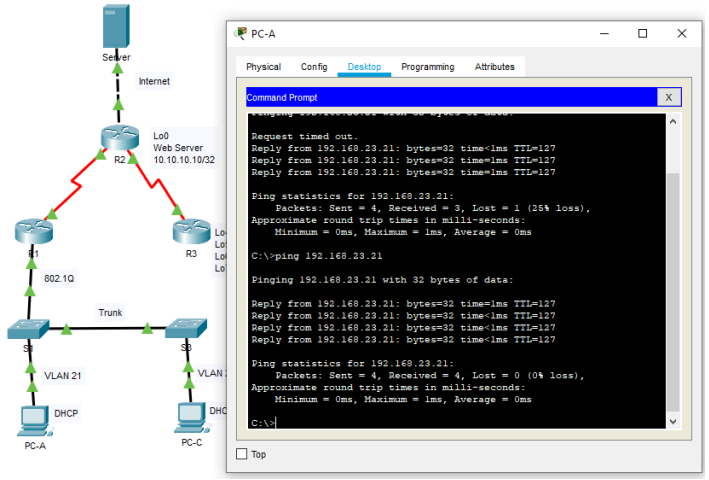



**Figura 6 - PING desde PC-A.**

CONFIGURACIÓN DE ACL.

Proceso para configurar las listas de control de acceso, se muestra a continuación:

| **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**<br>ip access-list standard ADMIN-MGT<br>permit host 172.16.1.1 |
| Aplicar la ACL con nombre a las líneas VTY | line vty 0 4<br>access-class ADMIN-MGT in<br>. |
| Permitir acceso por Telnet a las líneas de VTY | line vty 0 4<br>transport input telnet. |
| Verificar que la ACL funcione como se espera | show access-list. |

Tabla 6: ACL.

Verificamos la configuración realizada:

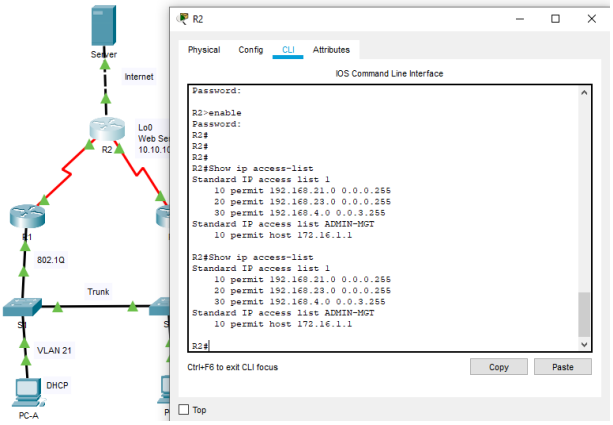



**Figura 7 - verificación de ACL EN R2**

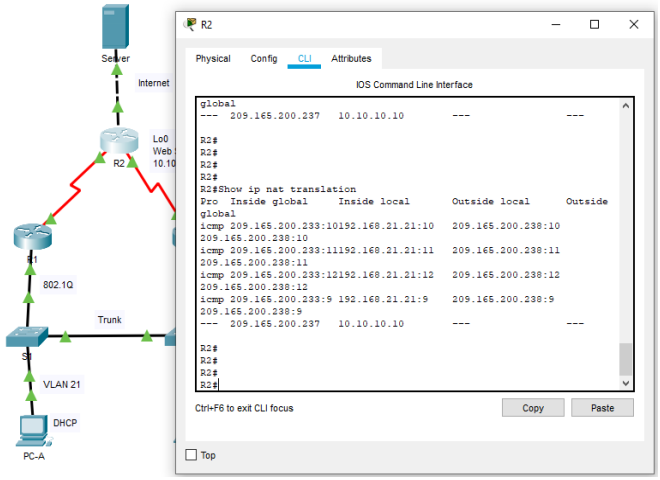



**Figura 8 - verificación NAT en R2.**

Referencias

[1] CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

[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

[3] Palta Velasco, E. (10 de Julio de 2014). INTRODUCCIÓN A LA SEGURIDAD EN REDES. Recuperado el 10 de Marzo de 2015, de http://datateca.unad.edu.co/contenidos/233010/UNIDAD_No1_SEGURIDAD_EN_REDES.pdf

[4] Maestros del Web.(19 de Agosto del 2003).Sistemas de detección de intrusos. Recuperado el 17 de Marzo del 2015, de http://www.maestrosdelweb.com

[5] W0LF_F4NG, 2020. Configuración Básica Ipv6 Router Cisco. [en línea] WF-Networking. Disponible en: https://www.w0lff4ng.org/configuracion-basica-ipv6-router-cisco/

[5] Willemvwyk, 2007. Err-Disabled On Fastethernet Port. [en linea] Community.cisco.com. Disponible en: https://community.cisco.com/t5/switching/err-disabled-on-fastethernet-port/td-p/716827

[6] Wikipedia, n.d. RSA. [en línea] Es.wikipedia.org. Disponible en: https://es.wikipedia.org/wiki/RSA

Biografía

John Jairo Ramirez Guevara nació en Barinas – Venezuela el 28 de mayo de 1981. Es graduado actualmente como tecnólogo en informática desde el 2006 título obtenido en Venezuela y también cuenta con el título de tecnólogo en Negocios Internacionales de Sena.
Actualmente se encuentra cursando la carrera de ingeniería de sistemas en la Universidad Nacional Abierta y a Distancia.
Su experiencia laboral abarca mas de 16 años, iniciándose como Técnico en computación en la empresa Básica, C.A. en Barinas Venezuela donde laboro hasta enero del 2015. Posteriormente laboro como Técnico de soporte en IBM en la ciudad de Cali en Colombia hasta mayo del 2016 y entre mayo del 2016 y noviembre del 2020 laboro en la empresa Juniper. S.A.S. donde ejerció las labores de Primary Support y Project Manager dando muy buena impresión por su labor como se evidencia en su promoción. Actualmente labora en la empresa Cafeto Software donde trabaja como Ingeniero de operaciones en un proyecto donde está creciendo profesionalmente.