# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNA

**MICHAEL DAVID GUERRA LIZARAZO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI**
**INGENIERÍA DE SISTEMAS**
**VALLEDUPAR**

**2020**

# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNA

**MICHAEL DAVID GUERRA LIZARAZO**

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

**DIRECTOR**

**DIEGO EDINSON RAMIREZ**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA DE SISTEMAS – VALLEDUPAR**
**2020**

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

VALLEDUPAR, 22 de mayo de 2020

# AGRADECIMIENTOS

Le agradezco a Dios por haberme acompañado y guido a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Le doy gracias a mis padres y hermanas por apoyarme en todo momento, por lo valores que me han inculcado, y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi carrera.

Le agradezco la confianza, el apoyo y la dedicación a mis profesores.

¡Muchas gracias por todo!

**CONTENIDO**

## LISTA DE TABLAS

## LISTA DE FIGURAS

## GLOSARIO

DNS (Nombre de dominio): traduce los nombres de hots a direcciones IP para ser entendidos por la computadora.

IP (Internet protocolo): es una dirección única que permite comunicación a la mayoría de redes.

Looback: Interface que dirige el tráfico hacia ellos mismos.

IPV4: Direcciones de 32 bits que se utiliza para identificar en dispositivo que está en una red.

IPV6: Direcciones de 128 bits, que se usa para identificar una red, es una actualización de las direcciones de IPV4.

## RESUMEN

Este diplomado se realiza para culminar la profundización de cisco, las practicas se desarrollaron en packet tracert que nos permitió crear los escenarios, los cuales nos pueden ayudar en nuestro entorno laboral aplicando estos conocimientos.

Este ejercicio tiene como objetivo solucionar dos escenarios seleccionados, se documentará cada paso de la configuración de los dispositivos en cada escenario de las redes, al final se verificará la conectividad por medio de comandos, se manejarán la conectividad de los equipos configurándolos con dirección ip e ipv6, con protocolos de enrutamiento dinámico, configuración ssh o telnet, configuración de DHCP y NAT, se configura NTP, se verifica la conectividad para dar solución a los ejercicios.



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



## ABSTRACT

This diploma is made to culminate the deepening of cisco, the practices were developed in packet tracert that allowed us to create the scenarios, which can help us in our work environment by applying this knowledge.

This exercise aims to solve two selected scenarios, each step of the configuration of the devices in each scenario of the networks will be documented, at the end the connectivity will be verified through commands, the connectivity of the equipment will be handled by configuring it with ip and ipv6 address, with dynamic routing protocols, ssh or telnet configuration, DHCP and NAT configuration, NTP configuration, the connectivity will be verified to give solution to the exercises.



Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

# INTRODUCCIÓN

Vivimos en un mundo donde todos los negocios no tienen los conocimientos suficientes para manejar las redes, por ese motivo es importante enseñarles las habilidades necesarias para que conozcan y adquieran conocimientos de cómo se configura el sistema de redes, logrando así una conectividad optima en las empresas.

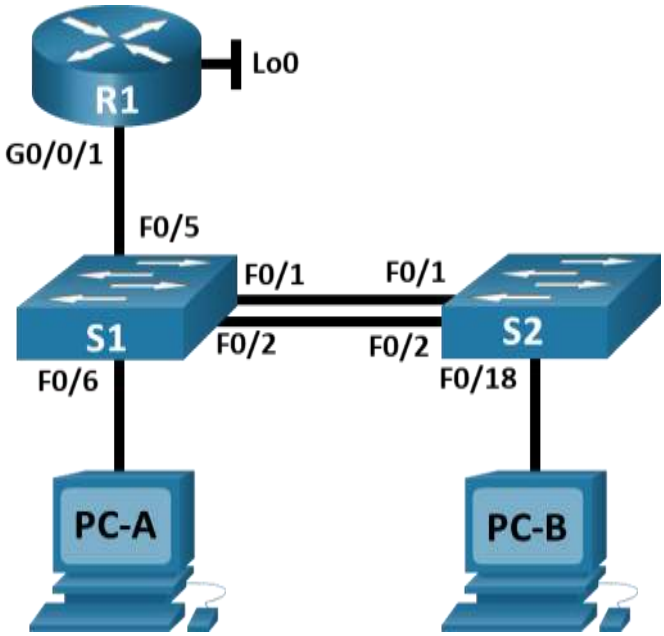
Mostraremos los conocimientos que un administrador en redes debe tener para cumplir los lineamientos de las topologías de red, mediante configuración e instalación, por lo tanto, se mejorarán las habilidades al mostrar la configuración de estos dos escenarios, mostrando los comandos más utilizados e importantes en el momento de realizar dicha actividad.

En el primer y segundo escenario se configurará una red pequeña donde se deberá configurar routers switch y equipos de cómputo que permitan y admitan conectividad ipv4 e ipv6 y sean seguros, con protocolos DHCP y protocolo en red NTP.

## DESARROLLO

1. ESCENARIO 1

*Figura 1. Escenario 1*




Se aprecia topología en Packet Tracer.

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. Tabla de Vlan*

Tabla de VLAN

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

*Tabla 2. Tabla de asignación de direcciones*

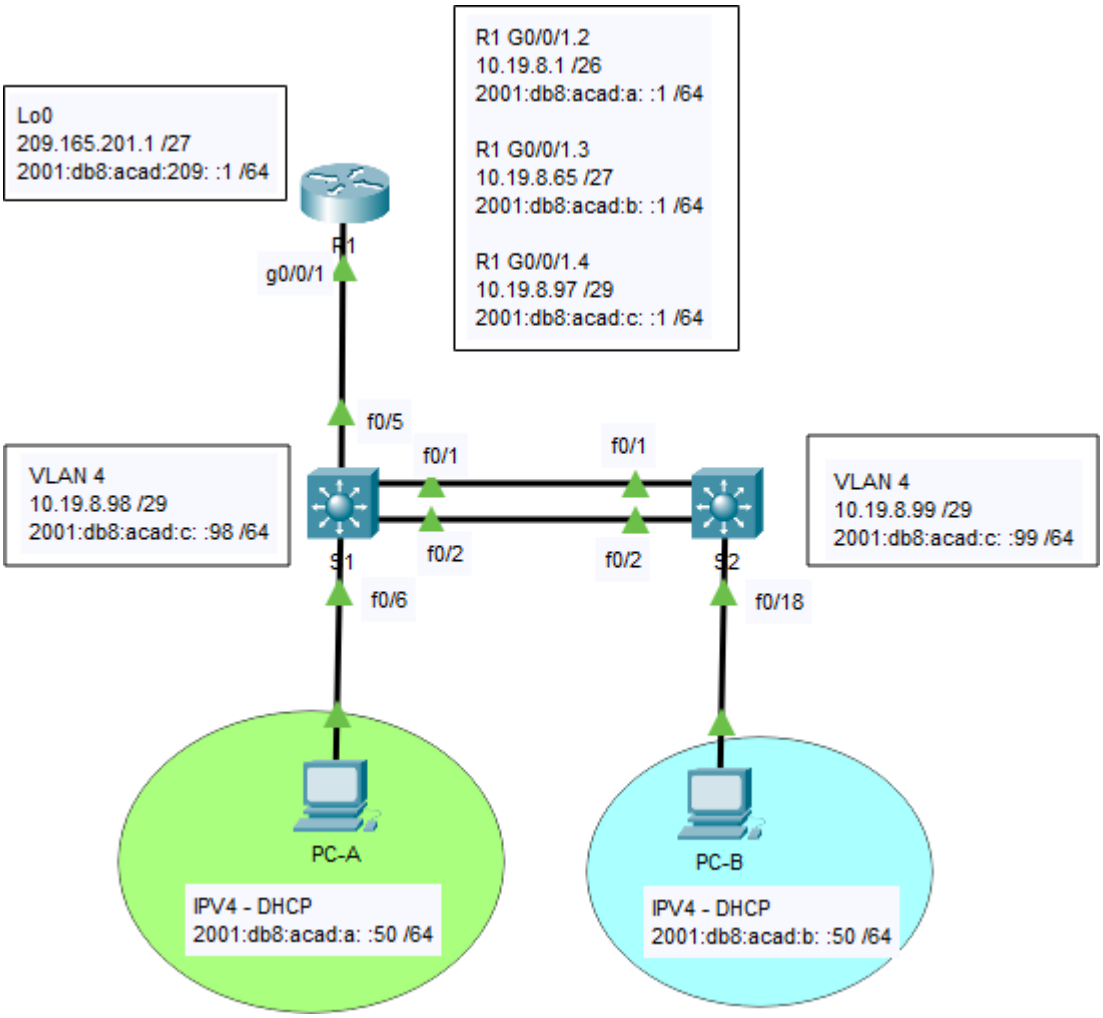
**Tabla de asignación de direcciones**

| 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 |
| 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 VLAN5.

Luego de conocer las IP que les vamos a asignar a cada uno de los dispositivos y sus interfaces y como conocemos la topología que vamos a armar podemos dejarlo indicado dentro de la misma, de esta manera es más sencillo su configuración y además las pruebas respectivas.

*Figura 2. Simulación del escenario*




*Nota: simulación realizada en CISCO Packet Tracer*

**Instrucciones**

**Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos**

**Paso 1: Inicializar y volver a cargar el router y el switch**

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.
- Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

*Tabla 3. Tarea Configurar R1*

**Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 3. Tarea Configurar R1*

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | **Empleamos para esto el siguiente commando:**<br><br>**Router(config)# no ip domain-lookup** |
| Nombre del router | Este lo debemos aplicar en cada uno de los ROUTERS.<br><br>**Router(config)#hostname R1** |
| Nombre de dominio | Como conocemos el nombre del dominio que vamos a configurar; ccna-lab.com debemos aplicar el siguiente comendo con el fin de poder crearlo.<br>**Router(config)# ip domain-lookup**<br>**Router(config)#ip domain-name ccna-lab.com** |
| Contraseña cifrada para el modo EXEC privilegiado | Estas es una de las partes más importantes en los dispositivos, debemos agregar seguridad a cada uno de los dispositivos, creamos la contraseña del modo EXEC, la contraseña a ingresar en cada uno de los dispositivos será: ciscoenpass<br><br>**enable secret ciscoenpass** |

| Tarea | Especificación |
| --- | --- |
| Contraseña de acceso a la consola | Igualmente, creamos las contraseñas que empleamos para el acceso a consola, en ese caso vamos a emplear: ciscoconpass. La forma de crear la misma es como indico a continuación.<br><br>**Router(config)#line con**<br>**Router(config)# password ciscoconpass**<br>**Router(config)#login** |
| Establecer la longitud mínima para las contraseñas | Podemos pedir que a la hora de crear las contraseñas mínimo tengan una longitud deseada: 10 caracteres para nuestro caso.<br><br>**Router(config)#security passwords min-length 10** |
| Crear un usuario administrativo en la base de datos local | Procedemos ahora a crear un usuario administrativo de la siguiente manera:<br><br>Nombre de usuario: **admin**<br>Password: **admin1pass**<br><br>Esto lo creamos empleando el siguiente comendo:<br><br>**username admin secret admin1pass** |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | El proceso de configuración de sesión de línea vty en ese caso sería:<br><br>**R1(config-line)#line vty 0 4**<br>**R1(config-line)#login local** |

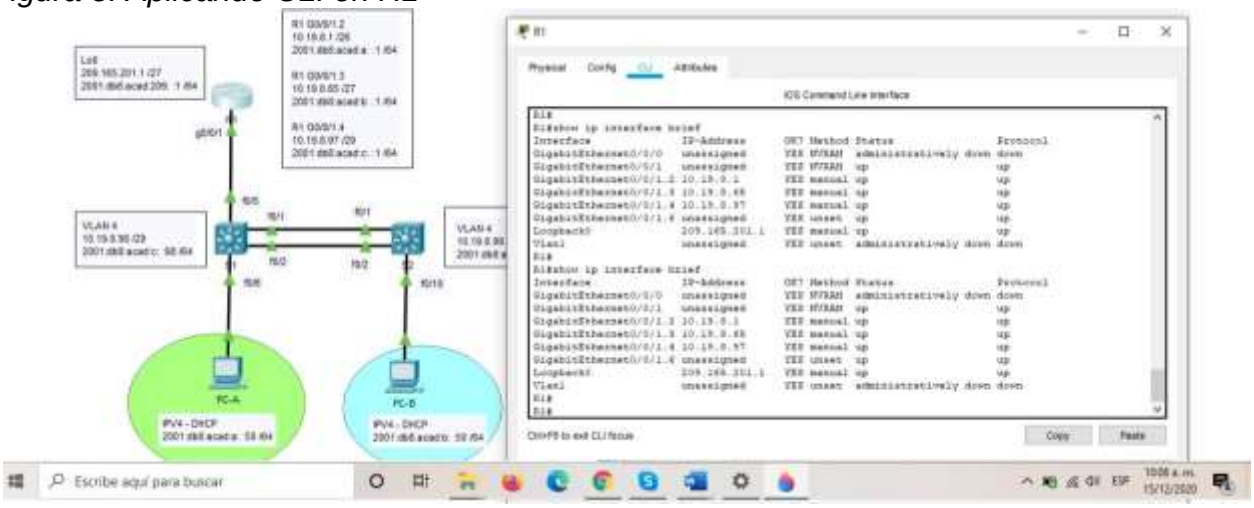
| Tarea | Especificación |
| --- | --- |
| Configurar VTY solo aceptando SSH | Para configurar esta laternativa se emplea el siguiente commando:<br><br>**R1(config-line)#line vty 0 4**<br>**transport input ssh** |
| Cifrar las contraseñas de texto no cifrado | Para poder encriptar las contraseñas con el fin de que estas no queden en texto, se emplea el siguiente comando:<br><br>**R1(config-line)#service password-encryption** |
| Configure un MOTD Banner | Este mensaje es muy empleado en los dispositivos, pues es la forma de persuader a las personas que quieran ingresar sin autorización.<br><br>**R1(config)#banner motd & SOLO PERSONAL AUTORIZADO &** |
| Habilitar el routing IPv6 | Activamos el enrutamiento IPV6<br><br>**R1(config)#ipv6 unicast-routing** |

| Tarea | Especificación |
| --- | --- |
| | Como siguiente punto debemos proceder a realizar la configuración de cada una de las interfaces que se nos indica en el cuadro anterior, debemos aparte de eso agregar información adicional que me permita conocer algo más con relación a la interfaz que estamos configurando.<br><br>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><br>R1(config-if)#interface GigabitEthernet0/0/1.2<br>R1(config-subif)#encapsulation dot1q 2<br>R1(config-subif)#description Bikes<br>R1(config-subif)#ip address 10.19.8.1 255.255.255.192<br>R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64<br>R1(config-subif)#ipv6 address FE80::1 link-local<br>R1(config-subif)#no shutdown<br>R1(config-subif)#interface GigabitEthernet0/0/1.3<br>R1(config-subif)#encapsulation dot1q 3<br>R1(config-subif)#description Trikes<br>R1(config-subif)#ip address 10.19.8.65 255.255.255.224<br>R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64<br>R1(config-subif)#ipv6 address FE80::1 link-local<br>R1(config-subif)#no shutdown<br>R1(config-subif)#interface GigabitEthernet0/0/1.4<br>R1(config-subif)#encapsulation dot1q 4<br>R1(config-subif)#description M1a8nagement<br>R1(config-subif)#ip address 10.19.8.97 255.255.255.248<br>R1(config-subif)#ipv6 address |

| Tarea | Especificación |
|---|---|
| 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 Loopback0<br>description Internet<br>R1(config-subif)#interface Loopback0<br>R1(config-if)#ip address 209.165.201.1 255.255.255.224<br>R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 |
| Generar una clave de cifrado RSA | Módulo de 1024 bits<br><br>**R1(config-if)#ipv6 address FE80::1 linklocal**<br>**R1(config-if)#no shutdown**<br>**R1(config-if)#**<br>Módulo de 1024 bits |

En esta tabla se aborda configuración en R1, se cambia el nombre del router, se le asigna una clave y posterior a eso un clave y además encriptada para dar Router (R1) seguridad

*Figura 3. Aplicando CLI en R1*



*Fuente: Autor*

Continuamos nuestro proceso, esta vez configurando los 2 SWITCHES.

*Tabla 4. Configure S1 y S2*

**Configure S1 y S2.**

Las tareas de configuración incluyen lo siguiente:

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS. | switch(config)#no ip domain-lookup |
| Nombre del switch | switch(config)#hostname R1 |
| Nombre de dominio | S1(config)#ip domain name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | **Ciscoenpass**<br>S1(config)#enable secret ciscoenpass<br>S1(config)#ip domain name ccna-lab.com |
| **Tarea** | **Especificación** |
| Contraseña de acceso a la consola | **Ciscoconpass**<br>S1(config)#line console 0<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login |
| Crear un usuario administrativo en la base de datos local | S1(config)#username admin password admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config-line)#line vty 0 15<br>S1(config-line)#login local<br>S1(config-line)#transport input ssh<br>S1(config-line)#exit |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S1(config)# ip ssh version 2<br>S1(config)# line vty 0 15<br>S1(config-line)# login local<br>S1(config-line)# exit |
| Cifrar las contraseñas de texto no cifrado | S1(config-line)#service password-encryption |

| | |
|---|---|
| Configurar un MOTD Banner | S1(config)#banner motd $Se prohibe el acceso no autorizado.$ |
| Generar una clave de cifrado RSA | S1(config)#ip domain-name span.com<br>S1(config)#crypto key generate rsa general-keys modulus 1024<br>S1(config)#username Bob secret cisco<br>S1(config)#line vty 0 4<br>S1(config-line)#login local<br>S1(config-line) #transport insut ssh<br>S1(config-line) #exit |
| | **S1**(config-if)#interface vlan4<br>s1(config-subif)#description Management<br><br>S1(config-if)#ip address 10.19.8.98 255.255.255.248<br>S1(config-if)#no shut<br>S1(config-if)#ip default-gateway 10.19.8.97<br>S1(config)#exit<br>S1(config-if)#ipv6 address 2001:db8:acad:c::98/64<br>S1(config-if)#ipv6 address FE80::98 link-local<br>S1(config-if)#no shutdown<br>S1(config-if)#end<br><br>**S2** |

| | |
|---|---|
| Configurar la interfaz de administración (SVI) | Switch>enable<br>Switch#configure terminal<br>Enter configuration commands, one per line. End with CNTL/Z.<br>Switch(config)#no ip domain-lookup<br>Switch(config)#hostname S2<br>S2(config)#ip domain name ccna-lab.com<br>S2(config)#enable secret ciscoenpass<br>S2(config)#line vty 0 15<br>S2(config-line)#password ciscoconpass<br>S2(config-line)#login<br>S2(config-line)#transport input ssh<br>S2(config-line)#exit<br>S2(config)#service password-encryption<br>S2(config)#banner motd #Unauthorized access is strictly prohibited. # |
| **Tarea** | **Especificación** |

| | |
|---|---|
| | S2(config)#crypto key generate rsa general-keys modulus 1024<br>The name for the keys will be: S2.ccna-lab.com<br><br>% The key modulus size is 1024 bits<br>% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]<br>*Mar 1 0:36:2.307: %SSH-5-ENABLED: SSH 1.99 has been enabled<br>S2#configure terminal<br>Enter configuration commands, one per line. End with CNTL/Z.<br>S2(config)#interface vlan4<br>S2(config-if)#description Management<br>S2(config-if)#ip address 10.19.8.99 255.255.255.248<br>S2(config-if)#no shutdown<br>S2(config-if)#ipv6 address 2001:db8:acad:c::99/64<br>S2(config-if)#ipv6 address FE80::99 link-local<br>S2(config-if)#no shutdown<br>S2(config-if)# |
| Configuración del gateway predeterminado | S1(config)# interface vlan1<br>S1(config-vlan)#ip address 10.19.8.97 255.255.255.0<br>S1(config-vlan)# no shut |

En esta tabla se deshabilita el DNS, cambiamos el nombre al switch por S1 & S2, y se crea un nombre de dominio llamdo ccna-lab.com, se crea contraseña para el modo EXEC y para acceso a consola y de paso son encriptadas, y si llegase a ver error de login se arroja un mensaje expresando “solo personal autorizado”, además se configura el cifrado RSA, interfaz (SVI) y configuración de Gateway.

**Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)**

**Configurar S1**

La configuración del S1 incluye las siguientes tareas:

*Tabla 5. Configure S1*

| Tarea | **Especificación** |
|---|---|
| Crear VLAN | Creamos cada una de las VLAN que se nos indica en el diagrama, junto con el nombre indicado:<br><br>S1(config)#vlan 2<br>S1(config-vlan)#name Bikes<br>S1(config-vlan)#vlan 3<br>S1(config-vlan)#name Trikes<br>S1(config-vlan)#vlan 4<br>S1(config-vlan)#name Management<br>S1(config-vlan)#vlan 5<br>S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Procedemos a configurar las interfaces y asignamos cada una de las interfaces a la VLAN correspondiente:<br><br>Interfaces F0/1, F0/2 y F0/5<br><br>S1#configure terminal<br>Enter configuration commands, one per line. End with CNTL/Z.<br>S1(config)#interface range f0/1-2<br>S1(config-if-range)#switchport trunk encapsulation dot1q<br>S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#<br>S1(config)#interface range f0/5<br>S1(config-if-range)#switchport trunk encapsulation dot1q<br>S1(config-if-range)#switchport trunk native vlan 6<br>S1(config-if-range)# |

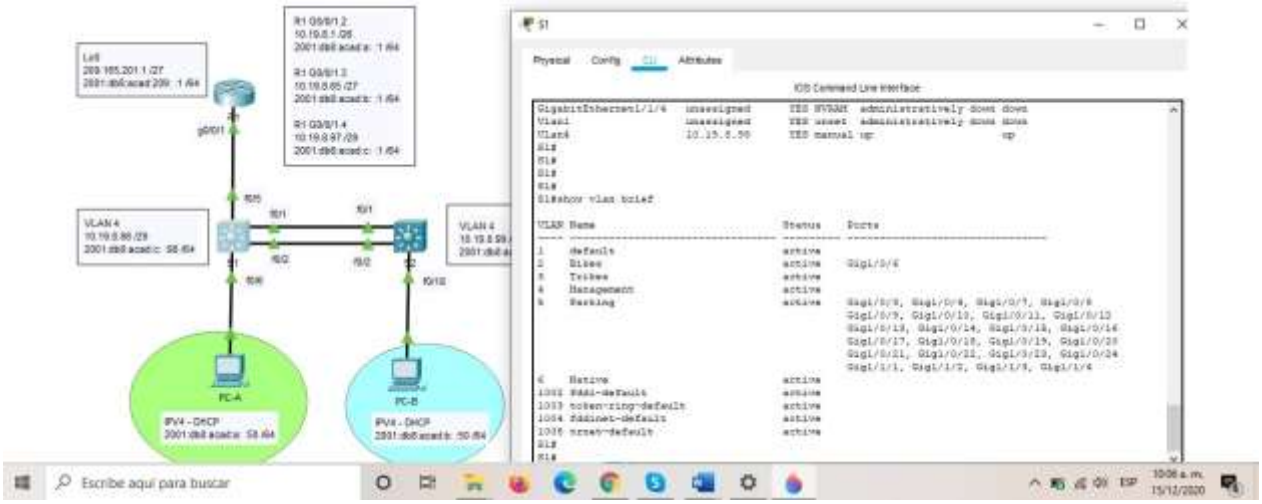
| Tarea | **Especificación** |
|---|---|
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | S1(config)#interface range f0/1-2<br>S1(config-if-range)#channel-group 1 mode active<br>S1(config-if-range)#<br>Creating a port-channel interface Port-channel 1<br>S1(config-if-range)#interface port-channel 1<br>S1(config-if)#switchport mode trunk<br>Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode..<br>S1(config-if)#switchport trunk native vlan 6<br>S1(config-if)# |
| Configurar el puerto de acceso de host para VLAN 2 | Interface F0/6<br>S1(config)#Interface F0/6<br>S1(config-if)#switchport mode access<br>S1(config-if)#switchport access vlan 2<br>S1(config-if)#<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down<br>S1(config-if)#switchport port-security<br>S1(config-if)# |
| Configurar la seguridad del puerto en los puertos de acceso | Permitir 3 direcciones MAC<br>Permitir 3 direcciones MAC<br>S1(config-if)#switchport port- security maximum 3**-security maximum 3** |

| Tarea | **Especificación** |
| --- | --- |
| Proteja todas las interfaces no utilizadas | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br><br>S1(config)#interface range f0/3-4<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description interface no use<br>S1(config-if-range)#no shutdown<br>S1(config)#interface range f0/7-24<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description interface no use<br>S1(config-if-range)#no shutdown<br>S1(config)#interface range g0/1-2<br>S1(config-if-range)#switchport mode access<br>S1(config-if-range)#switchport access vlan 5<br>S1(config-if-range)#description interface no use<br>S1(config-if-range)#no shutdown |

En esta tabla reflejada se crean las vlan (observe página 12), troncos para VLAN 6 nativa, y se aseguran todas las interfaces no utilizadas por seguridad

.

*Figura 4. Aplicando Código en S1*



*Fuente: Autor*

*Tabla 6. Configure S2*

**Configure el S2.**

**Entre las tareas de configuración de S2 se incluyen las siguientes:**

| Tarea | **Especificación** |
|---|---|
| Crear VLAN | Creamos las VLAN indicadas<br><br>S2(config)#vlan 2<br>S2(config-vlan)#name Bikes<br>S2(config-vlan)#vlan 3<br>S2(config-vlan)#name Trikes<br>S2(config-vlan)#vlan 4<br>S2(config-vlan)#name Management<br>S2(config-vlan)#vlan 5<br>S2(config-vlan)#name Parking<br>S2(config-vlan)#vlan 6<br>S2(config-vlan)#name Native |

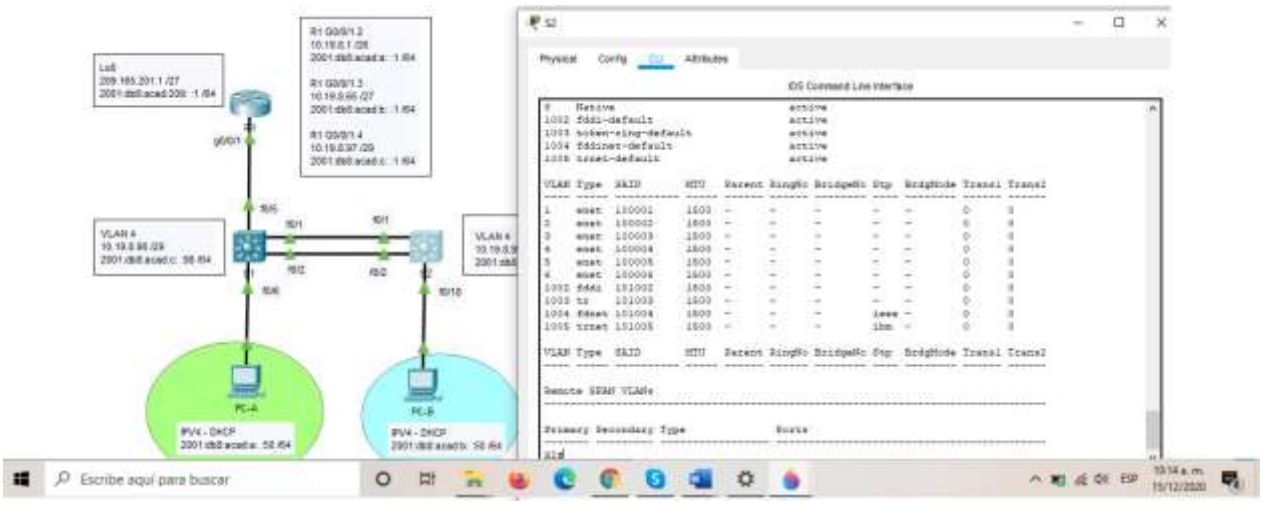
| Tarea | **Especificación** |
|---|---|
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Configuramos las interfaces solicitadas Interfaces F0/1 y F0/2<br><br>Interfaces F0/1 y F0/2<br>S2#configure terminal<br>Enter configuration commands, one per line. End with CNTL/Z.<br>S2(config)#interface range f0/1-2<br>S2(config-if-range)#switchport trunk encapsulation dot1q<br>S2(config-if-range)#switchport trunk native vlan 6<br>S2(config-if-range)# |
| 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>S2(config)#interface range f0/1-2<br>S2(config-if-range)#channel-group 1 mode active<br>S2(config-if-range)#Creating a port-channel interface Port-channel 1<br>S2(config-if-range)#interface port-channel 1<br>S2(config-if)#switchport mode trunk<br>S2(config-if)#switchport trunk native vlan 6<br>S2(config-if)# |
| Configurar el puerto de acceso del host para la VLAN 3 | Procedemos a configurar la Interfaz F0/18 y asignamos la misma a la VLAN 3.<br><br>Interfaz F0/18<br>S2(config)#Interface F0/18<br>S2(config-if)#switchport mode access<br>S2(config-if)#switchport access vlan 3<br>S2(config-if)#switchport port- security<br>S2(config-if)# |

| Tarea | **Especificación** |
| --- | --- |
| Configure port-security en los access ports | Procemos a configurar otro elemento de seguridad para nuestro dispotivios, en este caso permite 3 MAC addresses, esto lo podemos hacer con las MAC en específico o en su defecto dejando 3 MAC libres.<br><br>permite 3 MAC addresses permite 3 MAC addresses<br>S2(config-if)#switchport port- security maximum 3 |
| | Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar<br>S2(config)#Interface F0/18<br>S2(config-if)#switchport mode access<br>S2(config-if)#switchport access vlan 3<br>S2(config-if)#switchport port-security<br>S2(config-if)#switchport port-security maximum 3<br>S2(config-if)#exit<br>S2(config)#interface range f0/3-17<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description interface no use<br>S2(config-if-range)#no shutdown<br>S2(config-if-range)#<br>S2(config-if-range)#interface range f0/19-24<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description interface no use<br>S2(config-if-range)#no shutdown<br>S2(config-if-range)#<br>S2(config-if-range)#interface range |

| | |
|---|---|
| | g0/1-2<br>S2(config-if-range)#switchport mode access<br>S2(config-if-range)#switchport access vlan 5<br>S2(config-if-range)#description interface no use<br>S2(config-if-range)#no shutdown |
| Asegure todas las interfaces no utilizadas. | S2(config-if-range)# |

En esta tabla reflejada se crean las vlan (observe página 12), troncos para VLAN 6 nativa, y se aseguran todas las interfaces no utilizadas por seguridad

*Figura 5. Aplicando código en S2*



*Fuente: Autor*

Procedemos ahora a configurar el ROUTER R1

**Configurar soporte de host**

**Configure R1**

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 7. Configure R1 sobre host*

| Tarea | Especificación |
|---|---|
| Configure Default Routing | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0<br><br>R1(config)#Interface Loopback 0<br>R1(config-if)#Ip route 0.0.0.0<br>0.0.0.0 Loopback 0 R1(config)#Ipv6 route ::/0 Loopback 0<br>R1(config)# |
| 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>R1(config)#Ip dhcp pool vlan2-Bikes<br>R1(dhcp-config)#Network 10.19.8.0 255.255.255.192<br>R1(dhcp-config)#Domain- name ccna-a.net R1(dhcp-config)#Default- router 10.19.8.1<br>R1(dhcp-config)# |
| 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>R1(config)#Ip dhcp pool vlan3-Trikes<br>R1(dhcp-config)#Network 10.19.8.64 255.255.255.224<br>R1(dhcp-config)#Domain- name ccna-a.net R1(dhcp-config)#Default- router 10.19.8.65 |

Se crean rutas predeterminadas para IPv4 e IPV6 que dirijan el trafico hacia la interfaz Loopback 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, misma configuración para la VLAN 3

*Tabla 8. Configurar servidores*

**Configurar los servidores**

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUIA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**.

*Tabla 8.1. PC-A Network configuration*

| PC-A Network Configuration | |
|---|---|
| Descripción | PC-A<br>PC-A |
| Dirección física | 000A.F319.DABE |
| Dirección IP | 10.19.8.53<br>10.19.8.53 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.19.8.1 |
| Gateway predeterminado IPv6 | FE80::1 |

*Fuente: Autor*

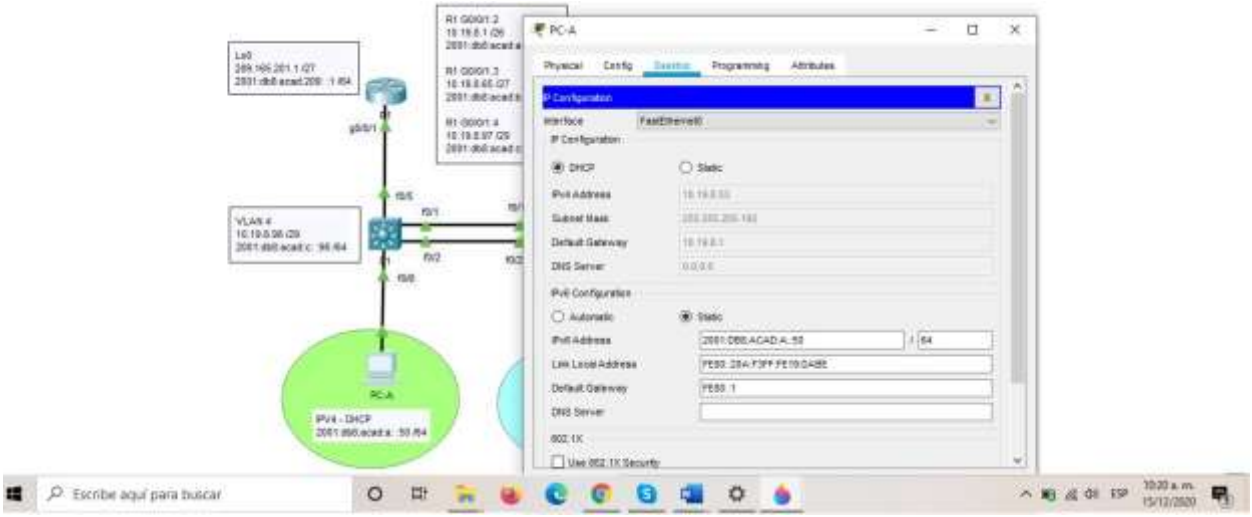
*Tabla 8.2. Configuración de red de PC-A*

| **Configuración de red de PC-A** | |
|---|---|
| Descripción | PC-A |
| Dirección física | 000A.F319.DABE |
| Dirección IP | 10.19.8.53 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.19.8.1 |
| Gateway predeterminado IPv6 | FE80::1 |

*Fuente: Autor*

*Tablas de información de cada PC y su direccionamiento.*

*Figura 6. Asignado ip pc-A*




*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:

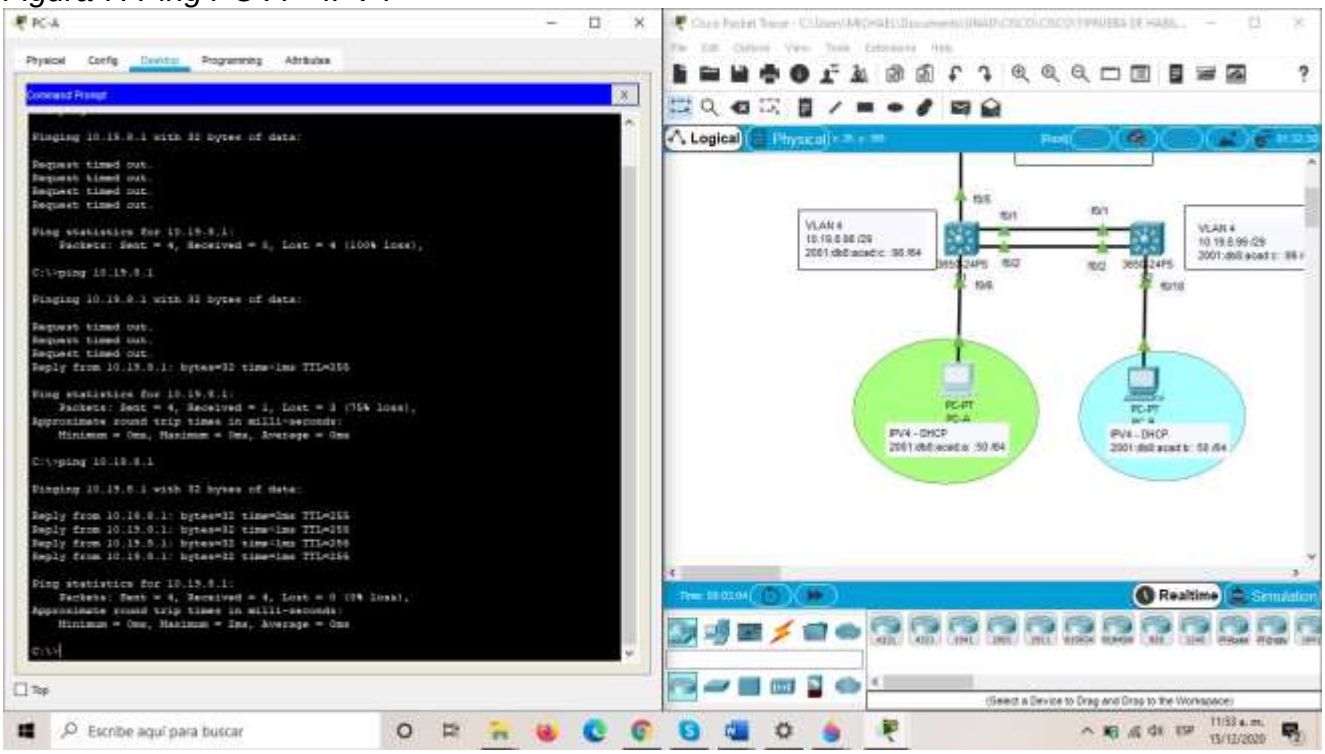
*Tabla 9. Probar y verificar la conectividad de extremo a extremo*

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-A | R1, G0/0/1.2 | Dirección | 10.19.8.1 | Exitoso |
| | | IPv6 | 2001:db8:acad:a: :1 | Exitoso |
| | | Dirección | 10.19.8.65 | Exitoso |
| | | IPv6 | 2001:db8:acad:b: :1 | Exitoso |
| | | Dirección | 10.19.8.97 | Exitoso |
| | | IPv6 | 2001:db8:acad:c: :1 | Exitoso |
| | | Dirección | 10.19.8.98 | Exitoso |
| | | IPv6 | 2001:db8:acad:c: :98 | Exitoso |
| | | Dirección | 10.19.8.99. | Exitoso |
| | | IPv6 | 2001:db8:acad:c: :99 | 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, 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 |

| Desde | A | de Internet | Dirección IP | Resultados de ping |
|---|---|---|---|---|
| PC-B | S2, VLAN 4 | Dirección | 10.19.8.99. | Exitoso |
| PC-B | S2, VLAN 4 | IPv6 | 2001:db8:acad:c::99 | Exitoso |

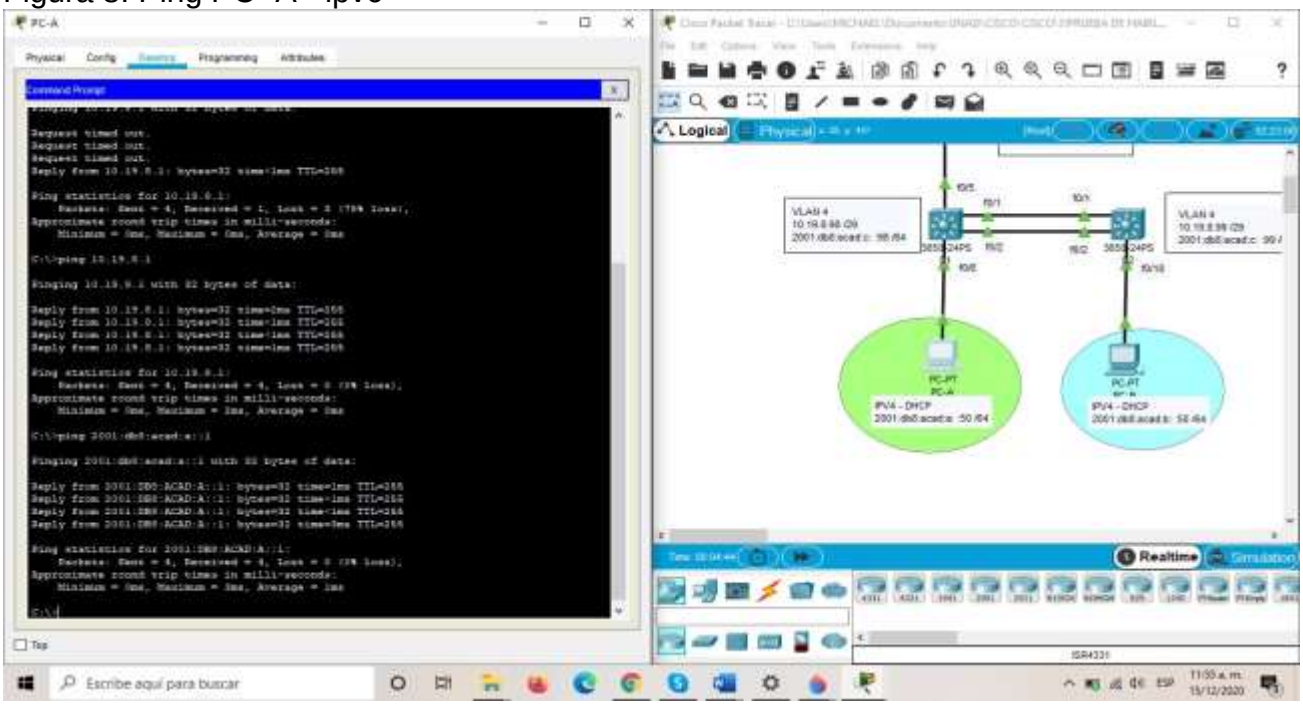
*Tabla demostrando Ping de manera exitosa*

*Figura 7. Ping PC-A – IPV4*



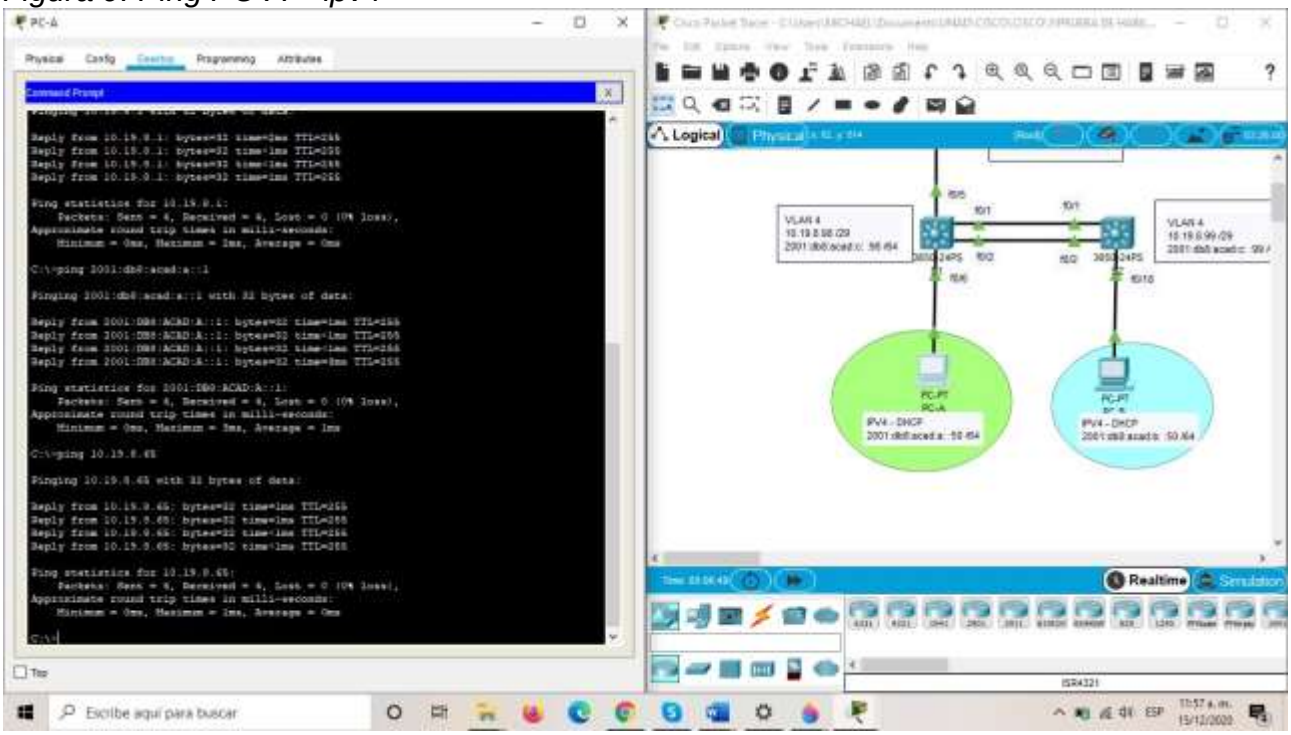

*Fuente: Autor*

Figura 8. Ping PC- A - ipv6



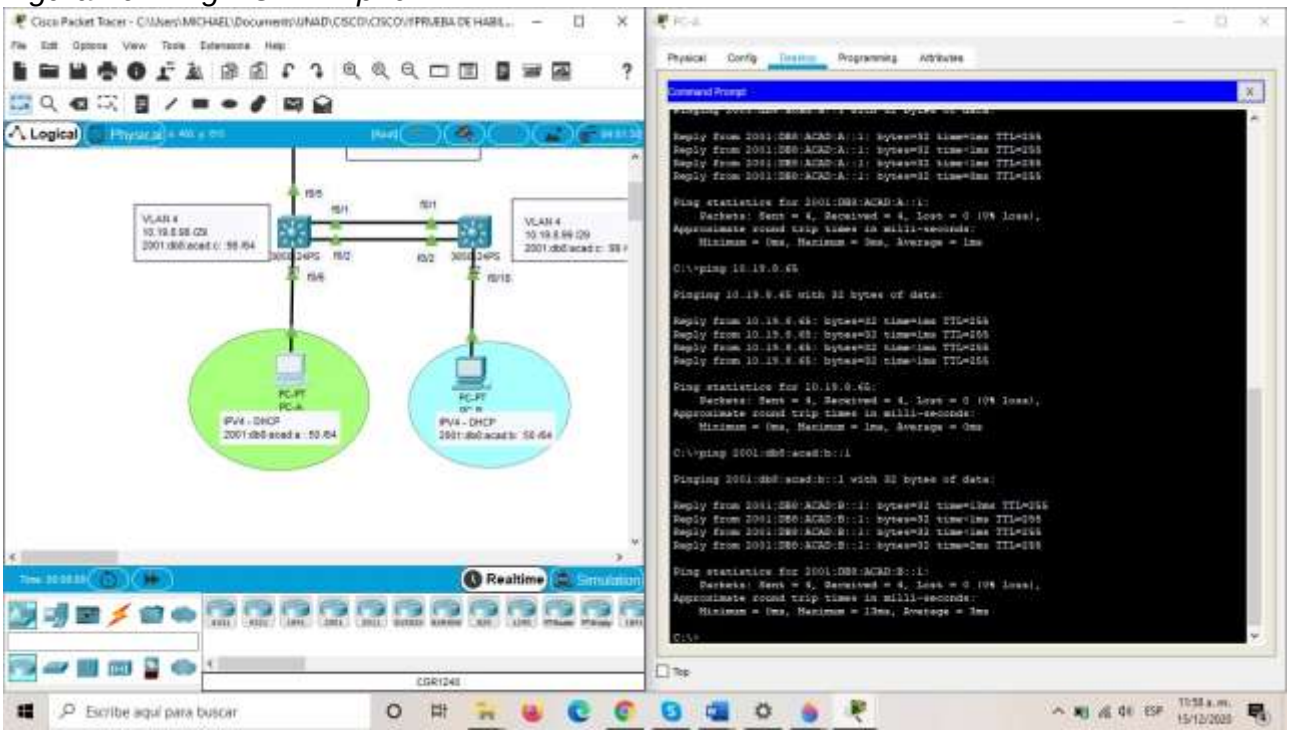
*Fuente: Autor*

*Figura 9. Ping PC-A – ipv4*



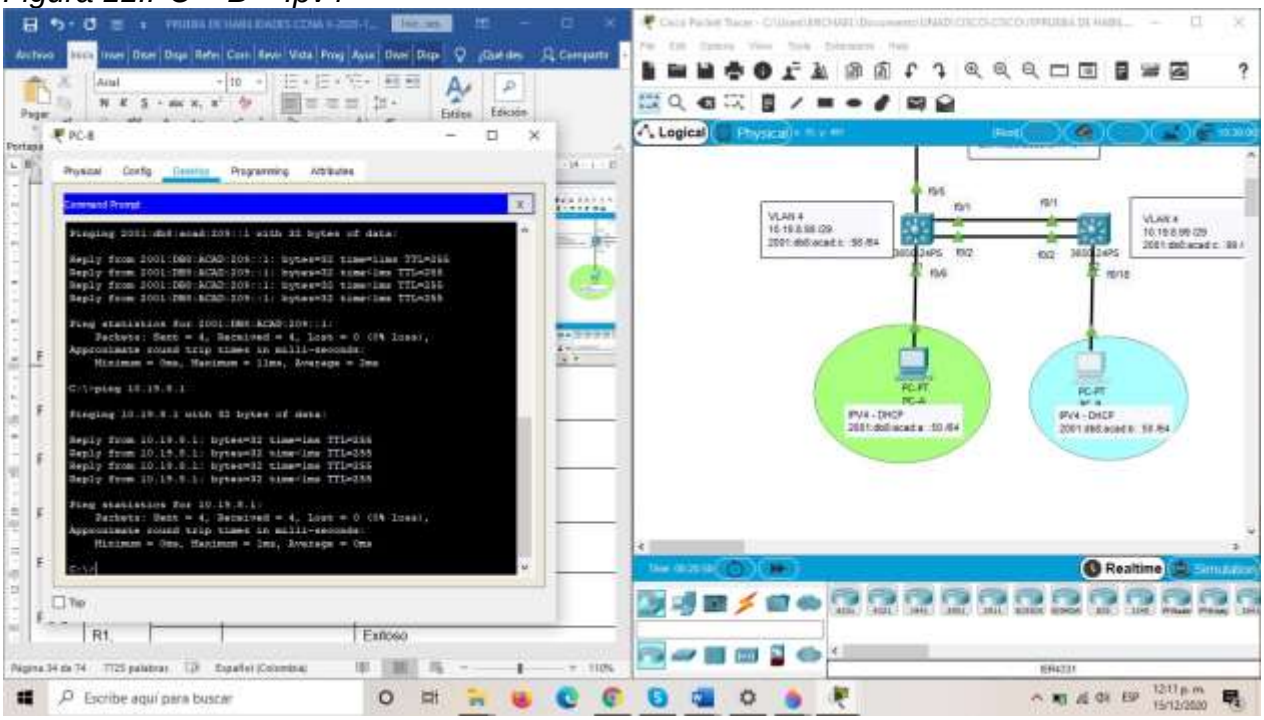
*Fuente: Autor.*

*Figura 10. Ping PC -A – ipv6*



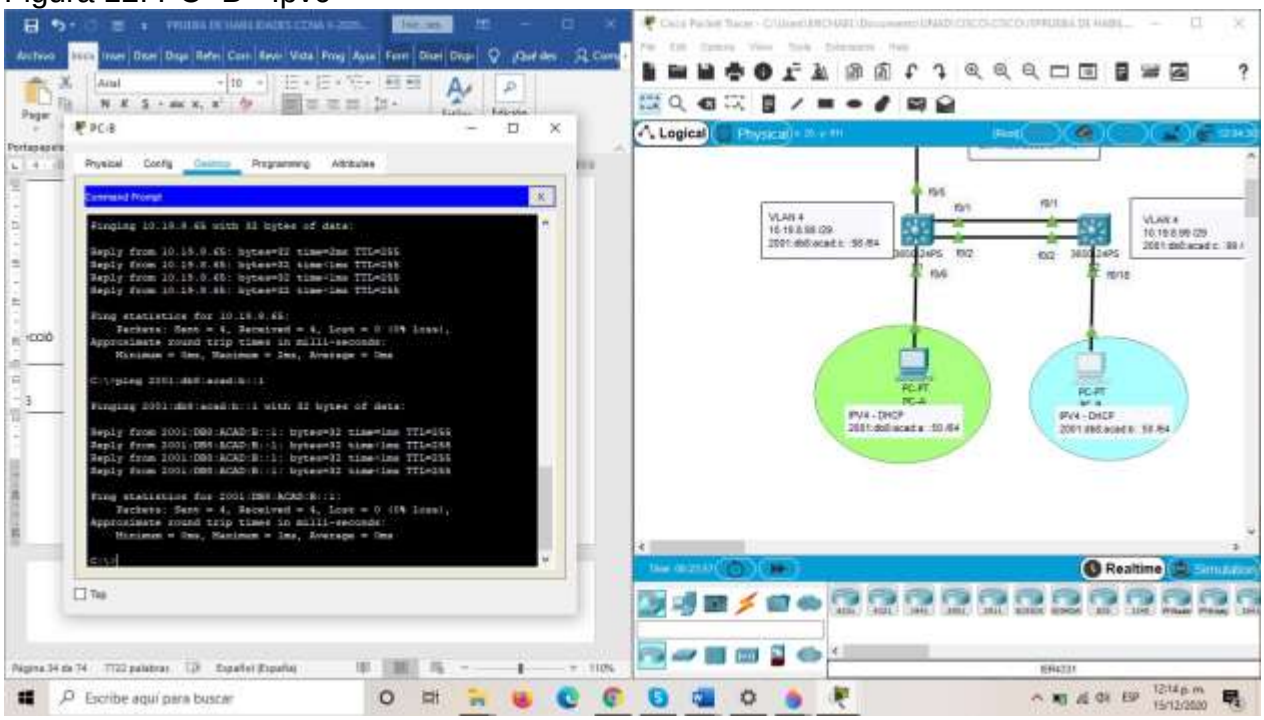
*Fuente: Autor*

*Figura 11.PC – B – Ipv4*



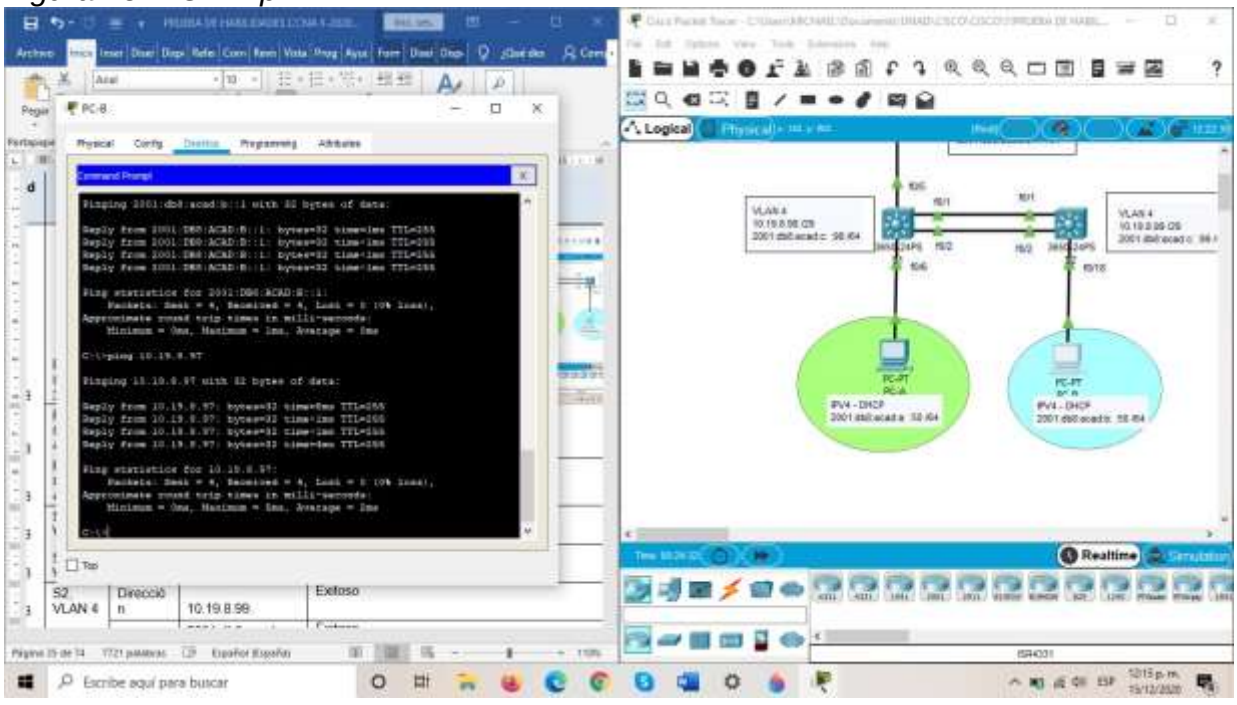
*Fuente: Autor*

Figura 12. PC- B - Ipv6



*Fuente: Autor*

*Figura 13. PC-B- ipv4*



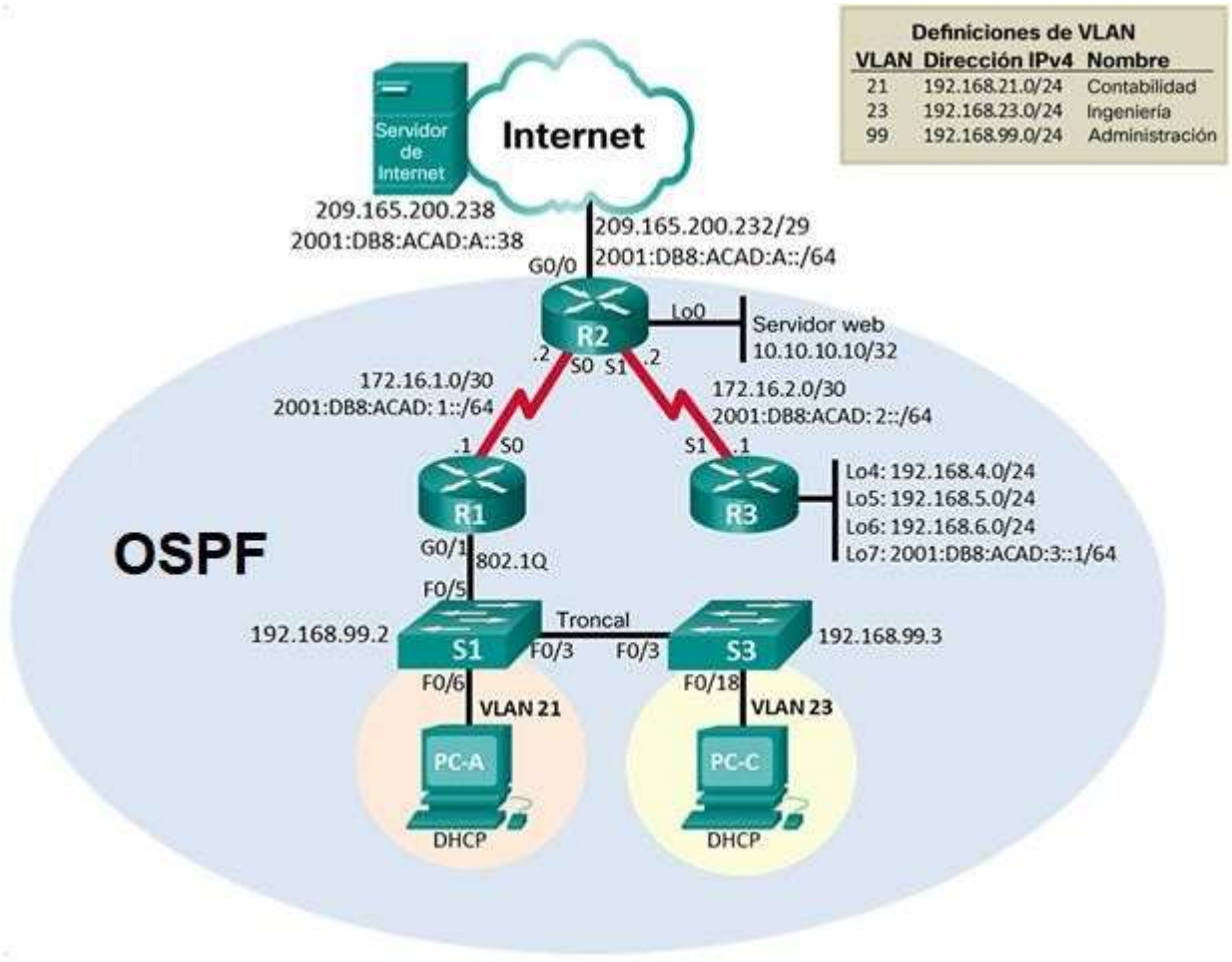
*Fuente: Autor*

**Escenario 2**

**Escenario: S**e 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.

Topología

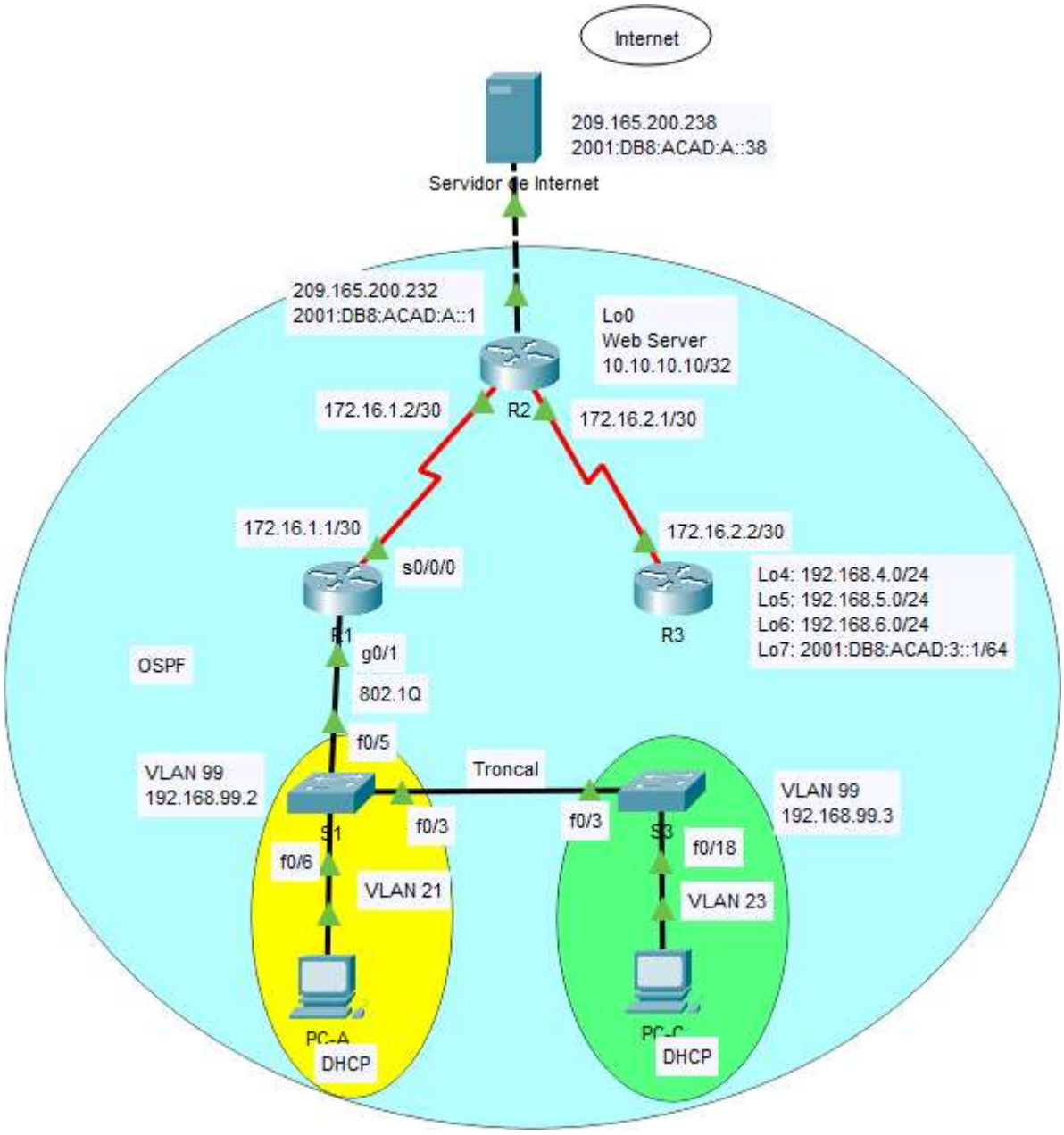
***Figura 14. Topología Escenario 2***




*Nota: Topologia realizada con CISCO Packet Tracer*

Procedemos a conectar la topoogía indicada.

*Figura 15. Topología conectada*




*Fuente: Autor*

**Inicializar dispositivos**

**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.

*Tabla 10. Inicializar y cargar los routers y los switches*

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Necesitamos eliminar toda la configuración del dispositivo, para esto empleamos el siguiente comando:<br>Router#erase startup-config |
| Volver a cargar todos los routers | Reiniciamos nuestro router,<br><br>Router#reload |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Para eliminar el archive start-up empleamos el siguiente commando en cada ROUTER Y SWITCH.<br><br>Switch#erase startup-config<br>Switch#delete vlan.dat |
| Volver a cargar ambos switches | Switch#reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Verificamos que los commando aplicados antes suerieron efecto**:**<br><br>Switch>enable<br>Switch#show flash |

En esta tabla se elimina toda la configuración del dispositivo, luego se reinicia el dispositivo, para eliminar la base de datos de VLAN y asi cargar los switch posteriormente detallamos que no esten en memoria flash

## Configurar los parámetros básicos de los dispositivos

### 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):

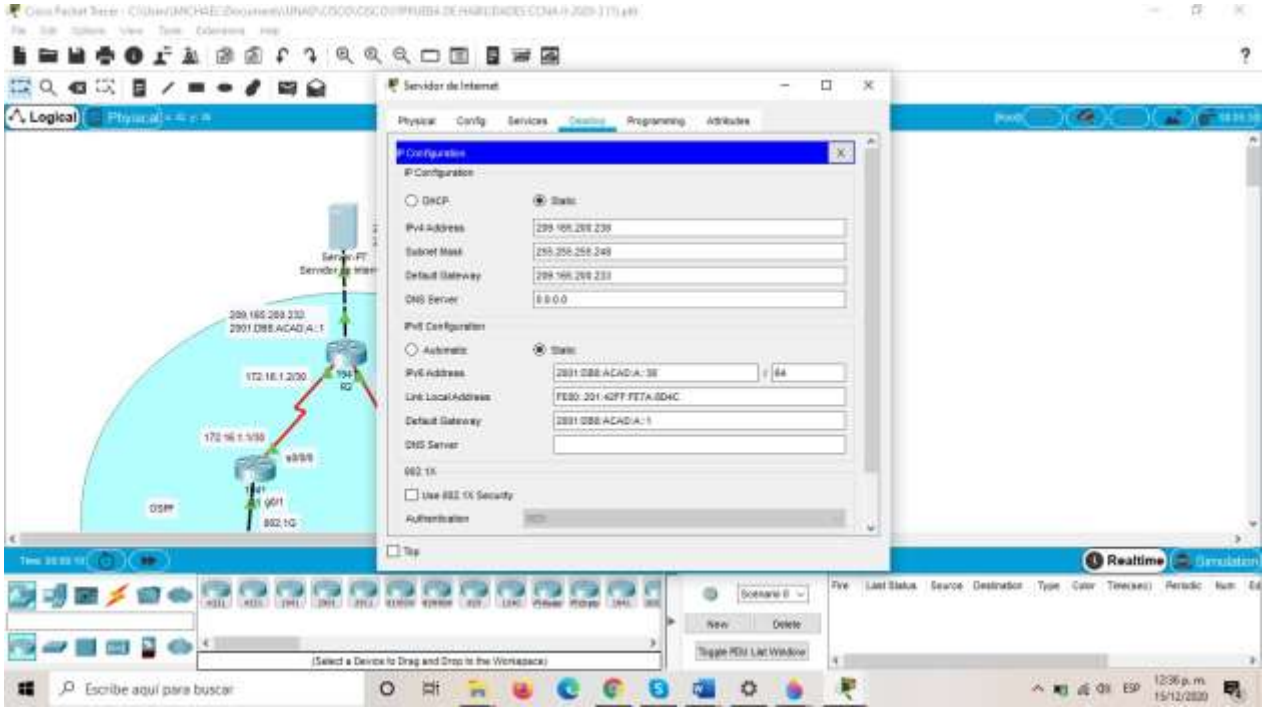
*Tabla 11. Configurar la computadora de internet*

| 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** |

*Tabla de direccionamiento*

**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.

*Figura 16. Dirección Ip de servidor de internet*




*Fuente: Autor*

**Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes

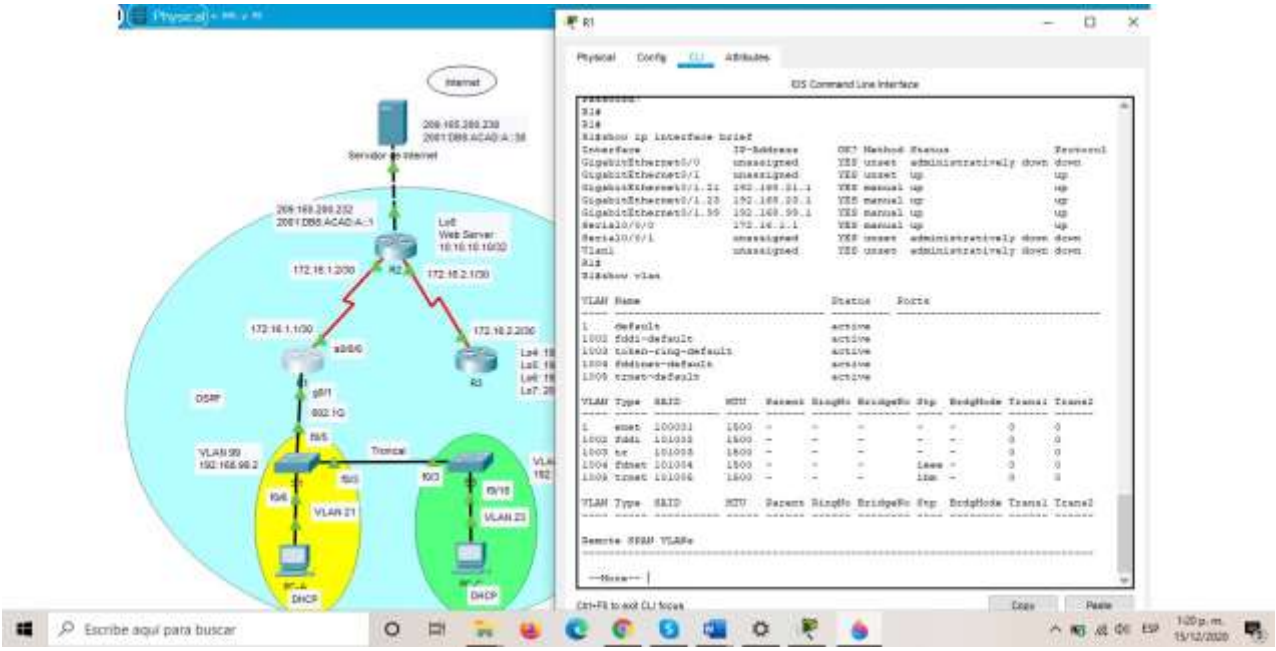
*Tabla 12. Configurar R1*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | *Para poder desactivar la busqueda DNS empleamos el siguiente comedo:*<br><br>Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | Agegamos la contraseña: class al modo exec provilegiado:<br><br>R1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | Configuramos la contraseña Cisco a consola:<br><br>R1(config)#line console 0<br>R1(config-line)#password ciscoconpass R1(config-line)#login |
| Contraseña de acceso Telnet | Configuramos la contraseña: cisco para la linea VTY.<br><br>R1(config-line)#line vty 0 4<br>R1(config-line)#password ciscoconpass R1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | *Debeos cifrar las contraseñas, esto con el fin de que no queden almacenas como texto, para ello empleamos el siguiente comando:*<br><br>R1(config)#service password-encryption |
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br><br>R1(config)#banner motd $Se prohibe el acceso no autorizado.$ |

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br>Establecer la dirección Ipv4 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la dirección Ipv6 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la frecuencia de reloj en 128000<br>Activar la interfaz<br><br>Interfaz S0/0/0<br>R1(config)#interface serial 0/0/0<br>R1(config-if)#description Connection to R2<br>R1(config-if)#ip address 172.16.1.1<br>255.255.255.252<br>R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no shutdown |
| Rutas predeterminadas | Configurar una ruta Ipv4 predeterminada de S0/0/0<br>Configurar una ruta Ipv6 predeterminada de S0/0/0<br><br>R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0<br>R1(config)#ipv6 route ::/0 s0/0/0 |

**Nota:** Todavía no configure G0/1, ya mencionado se desactiva la búsqueda DNS, se configura el nombre como R1, agregamos contraseñas para EXEC privilegiado y acceso a consola y una vez hecho se encriptan por seguridad. Se establece la dirección ipv4 e ipv6 (consulte tabla 11) y frecuencia de reloj en 128000, con rutas predeterminadas establecidas en la tabla 11.

*Figura 17. Configuración código R1*



*Fuente: Autor*

**Configurar R2**

La configuración del R2 incluye las siguientes tareas:

*Tabla 13. Configurar R2*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R2 |
| Contraseña de exec privilegiado cifrada | R2(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | R2(config)#line console 0<br>R2(config-line)#password ciscoconpass<br>R2(config-line)#login |
| Contraseña de acceso Telnet | R2(config-line)#line vty 0 4<br>R2(config-line)#password ciscoconpass<br>R2(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R2(config-line)#service password- encryption |
| Habilitar el servidor HTTP | R2(config)#ip http server |

| | |
|---|---|
| Mensaje MOTD | Se prohíbe el acceso no autorizado.<br><br>R2(config)#banner motd $Se prohibe el acceso no autorizado.$ |
| Interfaz S0/0/0 | Establezca la descripción<br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>Activar la interfaz<br><br>R2(config)#interface serial 0/0/0<br>R2(config-if)#description Connection to R1<br>R2(config-if)#ip address 172.16.1.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64<br>R2(config-if)#no shutdown |
| Interfaz S0/0/1 | Establecer la descripción<br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>Establecer la frecuencia de reloj en 128000.<br>Activar la interfaz<br><br>R2(config)#interface serial 0/0/1<br>R2(config-if)#description Connection to R3<br>R2(config-if)#ip address 172.16.2.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64<br>R2(config-if)#clock rate 128000 R2(config-if)#no shutdown |

| | |
|---|---|
| Interfaz G0/0 (simulación de Internet) | Establecer la descripción.<br>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.<br>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.<br>Activar la interfaz<br><br>R2(config)#interface gigabitEthernet 0/0<br>R2(config-if)#description Connection to Internet<br>R2(config-if)#ip address 209.165.200.233 255.255.255.248<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64<br>R2(config-if)#no shutdown |
| Interfaz loopback 0 (servidor web simulado) | Establecer la descripción.<br>Establezca la dirección IPv4.<br><br>R2(config-if)#Interface Loopback0<br>R2(config-if)#ip address 10.10.10.10 255.255.255.255 |
| Ruta predeterminada | Configure una ruta IPv4 predeterminada de G0/0.<br>Configure una ruta IPv6 predeterminada de G0/0.<br><br>R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0<br>R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 |

*En esta tabla de configuraciones de R2 se desactiva la busqueda de DNS, se cambia nombre del router 2 a R2, establecemos contraseñas para el EXEC privilegiado y modo consola y a su vez encriptadas, contraseña a telnet para acceder a interfaz virtual, habilitamos http para pruebas de internet, una vez luego modificando interfaz s0/0/0, 0/0/1, G0/0 que es la simulada de internet y lookback que sera el servidor web simulado*

*Figura 18. Configuracion codigo R2*

*Fuente: Autor*

**Configurar R3**

La configuración del R3 incluye las siguientes tareas:

*Tabla 14. Configurar R3*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R3<br>Router(config)#hostname R3 |
| Contraseña de exec privilegiado cifrada | R3(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | R3(config)#line console 0<br>R3(config-line)#password ciscoconpass<br>R3(config-line)#login |
| Contraseña de acceso Telnet | R3(config-line)#line vty 0 4<br>R3(config-line)#password ciscoconpass<br>R3(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R3(config-line)#service password-encryption |
| Mensaje MOTD | R3(config)#banner motd $Se prohibe el acceso no autorizado.$ |

| | |
|---|---|
| Interfaz S0/0/1 | R3(config)#interface serial 0/0/1<br>R3(config-if)#description Connection to R2<br>R3(config-if)#ip address 172.16.2.1 255.255.255.252<br>R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64<br>R3(config-if)#no shutdown |
| Interfaz loopback 4 | R3(config-if)#Interface Loopback4<br>R3(config-if)#ip address 192.168.4.1 255.255.255.0 |
| Interfaz loopback 5 | R3(config-if)#Interface Loopback5<br>R3(config-if)#ip address 192.168.5.1 255.255.255.0 |
| Interfaz loopback 6 | R3(config-if)#Interface Loopback6<br>R3(config-if)#ip address 192.168.6.1 255.255.255.0 |
| Interfaz loopback 7 | R3(config-if)#Interface Loopback7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 |
| Ruta predeterminada | R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1<br>R3(config)#ipv6 route ::/0 serial 0/0/1 |

*Tabla R3 se desactiva búsqueda DNS, nombre del router 3 pasa a ser R3 con su clave a EXEC privilegiado, a consola y telnet, una vez estas cifradas e encriptadas son su respectivo mensaje en lugar de error de acceso al loguearse; se establece la dirección ipv4 e ipv6 para activar interfazes s0/0/1 y interfaz subred como* Interfaz loopback 4, Interfaz loopback 5, Interfaz loopback 6, Interfaz loopback 7*, con sus ruta predeterminadas.*

**Configurar S1**

La configuración del S1 incluye las siguientes tareas:

*Tabla 15. Configurar S1*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del switch | Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | S1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | S1(config)#line console 0<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login |

| | |
|---|---|
| Contraseña de acceso Telnet | S1(config-line)#line vty 0 4<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | S1(config-line)#service password- encryption |
| Mensaje MOTD | S1(config)#banner motd $Se prohibe el acceso no autorizado.$ |

*Tabla de S1 se tiene en cuenta la desactivación de la busqueda DNS, se reescribe su nombre a S1, se anexan claves para el modo EXEC privilegiado, consola y acceso a telnet con su respectivo mensaje por si llega haber errores de logueo, y encriptadas por seguridad.*

**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:

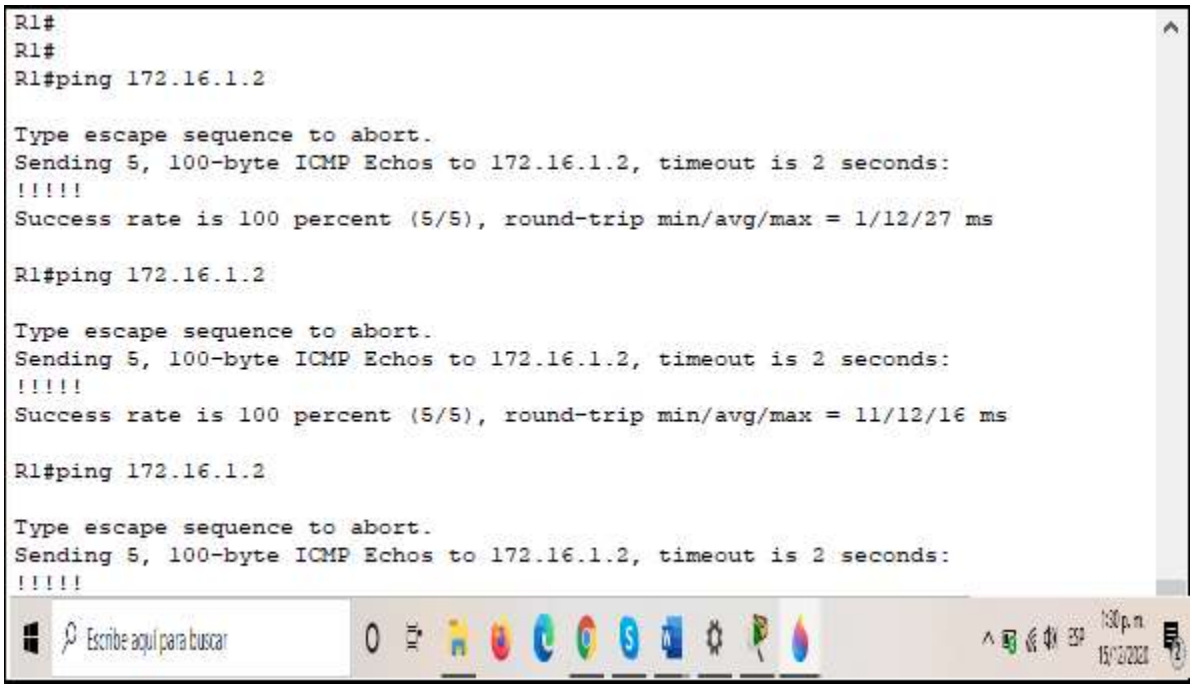
*Tabla 16. Verificar Red*

| Dede | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | *Observar figuras* |
| R2 | R3, S0/0/1 | 172.16.2.1 | *Observar figuras* |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | *Observar figuras* |

*Se utiliza el comando Ping para verificar conectividades, cuyo resultado fue exitoso (observe figuras 13 y figura 14).*

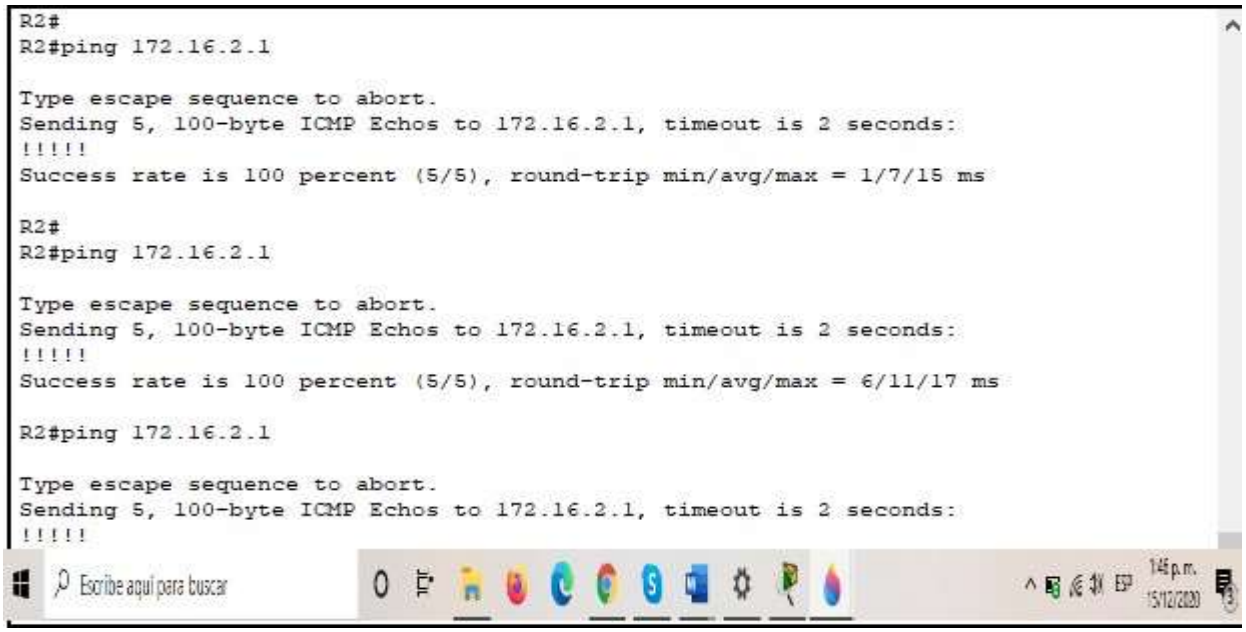
**Nota:** Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

*Figura 19. Ping R1*




*Fuente: Autor*

*Figura 20. Ping*




*Fuente: Autor*

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

**Configurar S1**

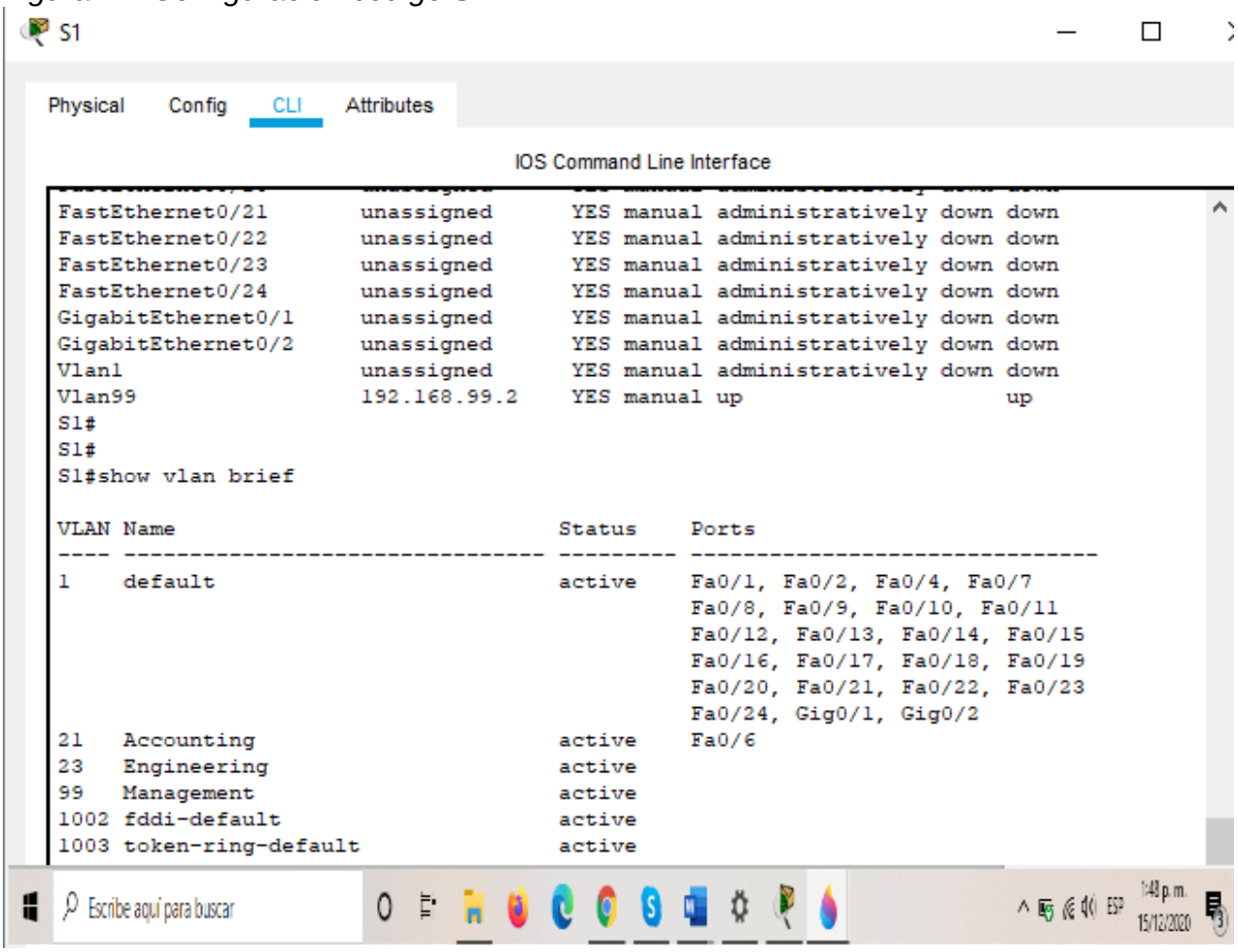
La configuración del S1 incluye las siguientes tareas:

*Tabla 17. Configurar S1-VLAN*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | S1(config)#vlan 21<br>S1(config-vlan)#name Contabilidad<br>S1(config-vlan)#vlan 23<br>S1(config-vlan)#name Ingenieria<br>S1(config-vlan)#vlan 99<br>S1(config-vlan)#name Administracion |
| Asignar la dirección IP de administración. | S1(config)#interface vlan 99<br>S1(config-if)#ip address 192.168.99.2 255.255.255.0<br>S1(config-if)#no shutdown |
| Asignar el gateway predeterminado | S1(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Forzar el enlace troncal en la interfaz F0/5 | S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S1(config-if)#interface range f0/1-2, f0/4, f0/6- 24, g0/1-2<br>S1(config-if-range)#switchport mode access |
| Asignar F0/6 a la VLAN 21 | S1(config-if-range)#interface fastEthernet 0/6<br>S1(config-if)#switchport access vlan 21 |
| Apagar todos los puertos sin usar | S1(config-if)#interface range f0/1-2, f0/4, f0/7- 24, g0/1-2<br>S1(config-if-range)#shutdown |

*Se crean las bases de datos contabilidad, ingeniería y administración, se asigna direcciones ipv4 a la vlan de administración y usamos la* IP asignada al S1 en el diagrama de topología, se asignan el Gateway predeterminado y se fuerzan troncales F/03, F/05, se configuran el resto de puertos como puertos de acceso y apagamos los sin usar por seguridad.

*Figura 21. Configuración código S1*




*Fuente: Autor*

**Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

*Tabla 18. Configurar S3-VLAN*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | S3(config)#vlan 21<br>S3(config-vlan)#name Contabilidad<br>S3(config-vlan)#vlan 23<br>S3(config-vlan)#name Ingenieria<br>S3(config-vlan)#vlan 99<br>S3(config-vlan)#name Administracion |
| Asignar la dirección IP de administración | S3(config-vlan)#interface vlan 99<br>S3(config-if)#ip address 192.168.99.3 255.255.255.0<br>S3(config-if)#no shutdown |

| | |
|---|---|
| Asignar el gateway predeterminado. | S3(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S3(config)#interface range f0/1-2, f0/4-24, g0/1-2<br>S3(config-if-range)#switchport mode access |
| Asignar F0/18 a la VLAN 23 | S3(config-if-range)#interface fastEthernet 0/18<br>S3(config-if)#switchport access vlan 23 |
| Apagar todos los puertos sin usar | S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2<br>S3(config-if-range)#shutdown |

*Se crean las bases de datos contabilidad, ingeniería y administración, se asigna direcciones ipv4 a la vlan de administración y usamos la* IP asignada al S1 en el diagrama de topología, se asignan el Gateway predeterminado y se fuerzan troncales F/03, F/05, se configuran el resto de puertos como puertos de acceso y apagamos los sin usar por seguridad y por último se asigna $F0/18$ a la VLAN 23

**Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 19. Configurar R1*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | R1(config)#interface gigabitEthernet 0/1.21<br>R1(config-subif)#description LAN de Contabilidad<br>R1(config-subif)#encapsulation dot1Q 21<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | R1(config-subif)#interface gigabitEthernet 0/1.23<br>R1(config-subif)#description LAN de Ingenieria<br>R1(config-subif)#encapsulation dot1Q 23<br>R1(config-subif)#ip address 192.168.23.1 255.255.255.0 |

| | |
|---|---|
| Configurar la subinterfaz 802.1Q .99 en G0/1 | R1(config-subif)#interface gigabitEthernet 0/1.99<br>R1(config-subif)#description LAN de Administracion<br>R1(config-subif)#encapsulation dot1Q 99<br>R1(config-subif)#ip address 192.168.99.1 255.255.255.0 |
| Activar la interfaz G0/1 | R1(config-subif)#int g0/1<br>R1(config-if)#no shutdown |

Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz, Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz, Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz

**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:

*Tabla 20. Verificar la red*

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | *192.168.99.1* | *Observar figuras* |
| S3 | R1, dirección VLAN 99 | *192.168.99.1* | *Observar figuras* |
| S1 | R1, dirección VLAN 21 | *192.168.21.1* | *Observar figuras* |
| S3 | R1, dirección VLAN 23 | *192.168.23.1* | *Observar figuras* |

*Tabla donde se verifica conectividad de red y son exitosas*

*Figura 22. Ping S1*


*Fuente: Autor*

*Figura 23. Ping S3*

*Fuente: Autor*

**Configurar el protocolo de routing dinámico OSPF**

**Configurar OSPF en el R1**

Las tareas de configuración para R1 incluyen las siguientes:

*Tabla 21. Configurar OSPF en el R1*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)#router ospf R2(config-router)#version 3 |

| | |
|---|---|
| Anunciar las redes conectadas directamente | R1(config-router)#do show ip route connected<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21<br>C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23<br>C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99<br>R1(config-router)#network 172.16.1.0<br>R1(config-router)#network 192.168.21.0<br>R1(config-router)#network 192.168.23.0<br>R1(config-router)#network 192.168.99.0 |
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface gigabitEthernet 0/1.21<br>R1(config-router)#passive-interface gigabitEthernet 0/1.23<br>R1(config-router)#passive-interface gigabitEthernet 0/1.99 |
| Desactive la sumarización automática | R1(config-router)#no auto-summary |

*Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 18) y establecemos interfaces LAN como pasivas.*

*Figura 24. Correcta configuración de R1-OSPF*


*Fuente: Autor.*

**Configurar OSPF en el R2**

La configuración del R2 incluye las siguientes tareas:

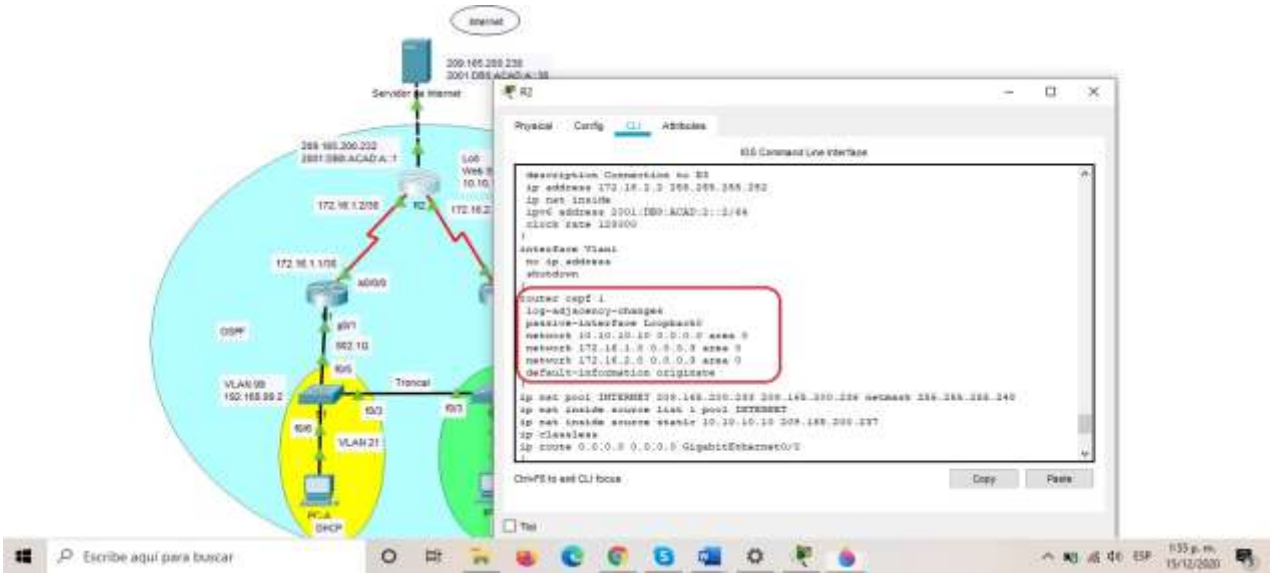
*Tabla 22. Configurar OSPF en el R2*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)#router osfp R2(config-router)#version 3 |

| | |
|---|---|
| Anunciar las redes conectadas directamente | R2(config-router)#do show ip route connected<br>C 10.10.10.10/32 is directly connected, Loopback0<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 209.165.200.232/29 is directly connected, GigabitEthernet0/0<br>R2(config-router)#network 10.10.10.10<br>R2(config-router)#network 172.16.1.0<br>R2(config-router)#network 172.16.2.0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface loopback 0 |
| Desactive la sumarización automática. | R2(config-router)#no auto-summary |

*Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 19) y establecemos interfaces LAN como pasivas.*

*Figura 25. Correcta configuración de R2-OSPF*



*Fuente: Autor.*

**Configurar OSPFv3 en el R3**

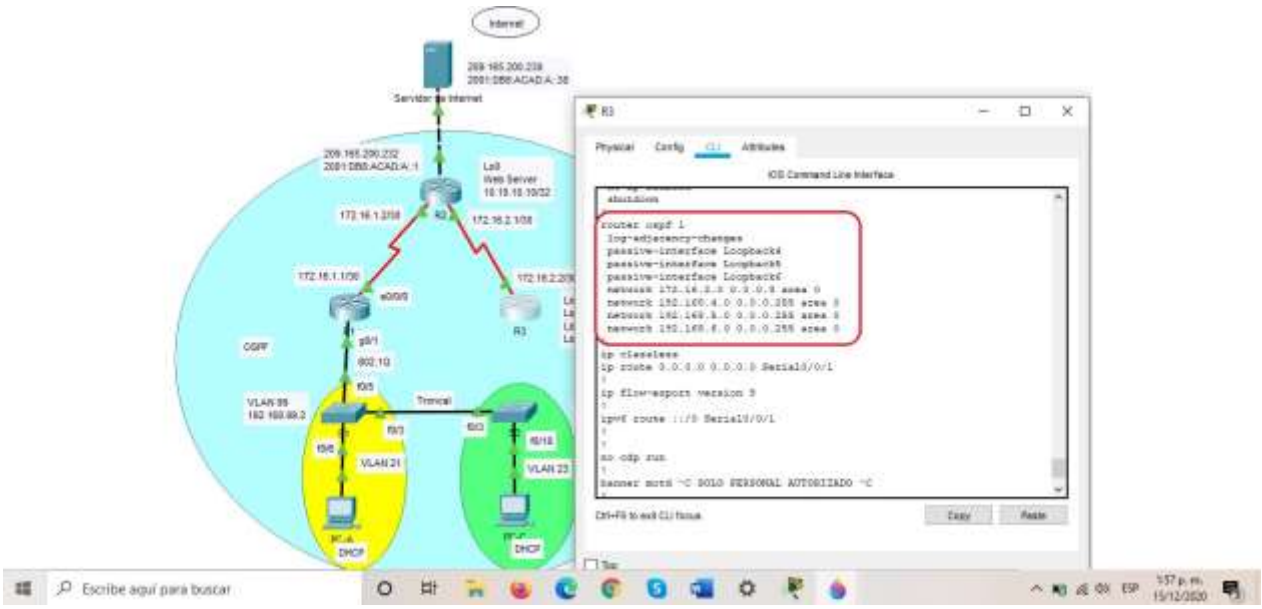
La configuración del R3 incluye las siguientes tareas:

*Tabla 23. Configurar OSPFv3 en el R3*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)# ipv6 router ospf 1<br>R3(config-rtr)# router-id 3.3.3.3 |
| Anunciar redes IPv4 conectadas directamente | R2(config-router)#do show ip route connected<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 192.168.4.0/24 is directly connected, Loopback4<br>C 192.168.5.0/24 is directly connected, Loopback5<br>C 192.168.6.0/24 is directly connected, Loopback6<br>R2(config-router)#network 172.16.2.0<br>R2(config-router)#network 192.168.4.0<br>R2(config-router)#network 192.168.5.0<br>R2(config-router)#network 192.168.6.0 |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R2(config-router)#passive- interface loopback 4<br>R2(config-router)#passive- interface loopback 5<br>R2(config-router)#passive- interface loopback 6 |
| Desactive la sumarización automática. | R2(config-router)#no auto-summary |

*Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 20) y establecemos interfaces LAN como pasivas*

*Figura 26. Correcta configuración de R3-OSPF*




*Fuente: Autor*

**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 24. Verificar información de OSPF*

| Pregunta | Respuesta |
|---|---|
| R2#show ip route ospf | R2#show ip protocols |
| ¿Qué comando muestra solo las rutas OSPF? | R2#show ip route ospf |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | R2#show run \| section router ospf<br>router ospf |

*Tabla de preguntas y/o aclaración de dudas*

**Implementar DHCP y NAT para IPv4**

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

Las tareas de configuración para R1 incluyen las siguientes:

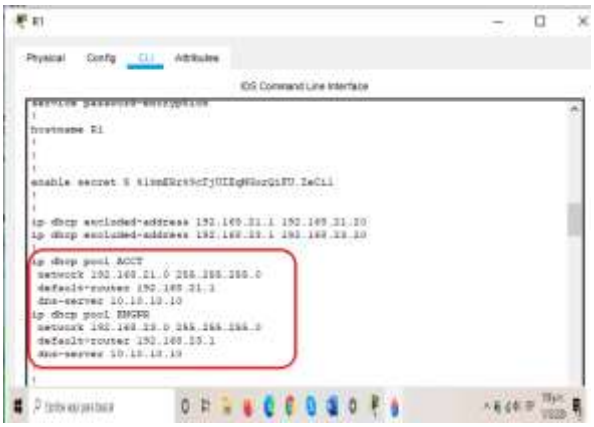
*Tabla 25. Implementar DHCP y NAT para IPV4*

| Elemento o tarea de configuración | Especificación |
|---|---|

| | |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |
| Crear un pool de DHCP para la VLAN 21. | Nombre: ACCT<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado<br><br>R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br>R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 |
| 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>R1(dhcp-config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#network 192.168.23.0 255.255.255.0<br>R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 |

*Reservamos las primeras 20 direcciones ip en la VLAN 21 para configuraciones estáticas* Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crea un pool de DHCP para la VLAN 21. Y por ultimo Crear un pool de DHCP para la VLAN 23

*Figura 27. Configuración R1 Ip DHCP POOL.*



*Fuente: Autor*

**Configurar la NAT estática y dinámica en el R2**

La configuración del R2 incluye las siguientes tareas:

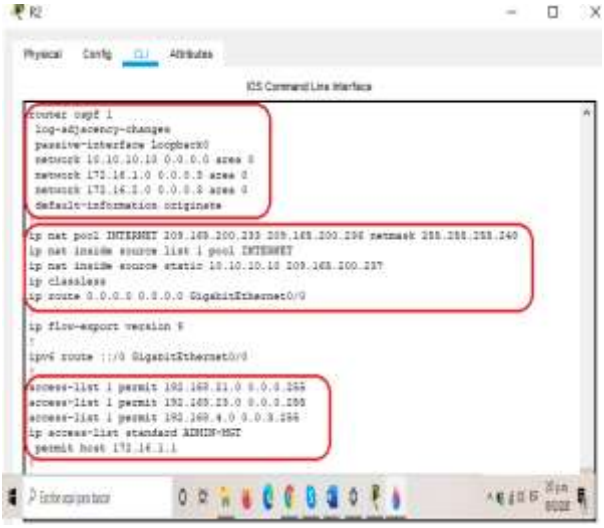
*Tabla 26. Configurar la NAT estática y dinámica en el R2*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | Nombre de usuario: **webuser**<br>Contraseña: **cisco12345**<br>Nivel de privilegio: **15**<br><br>R2(config)#username webuser privilege 15 secret cisco12345 |
| Habilitar el servicio del servidor HTTP | R2(config)#ip http server |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config)#ip http authentication local |
| Crear una NAT estática al servidor web. | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 |
| Asignar la interfaz interna y externa para la NAT estática | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 |
| Configurar la NAT dinámica dentro de una ACL privada | R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 |

| | |
|---|---|
| Defina el pool de direcciones IP públicas utilizables. | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3<br><br>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

*Se* crea una base de datos local con una cuenta de usuario, se habilita el servicio de servidor http se configura para autenticar, una vez hecho se crea la NAT estatica a dicho servidor web se le asigan interfaces internas y externas.

*Figura 28. Configuración NAT en R2.*



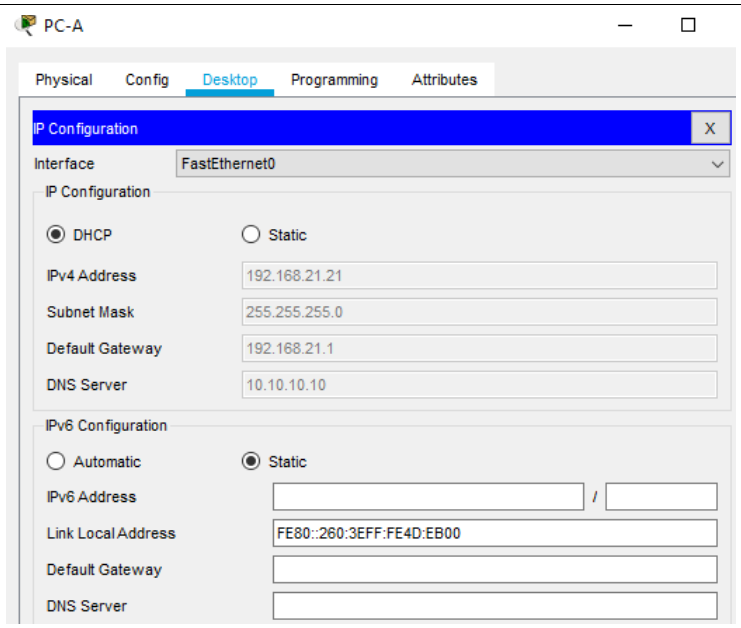
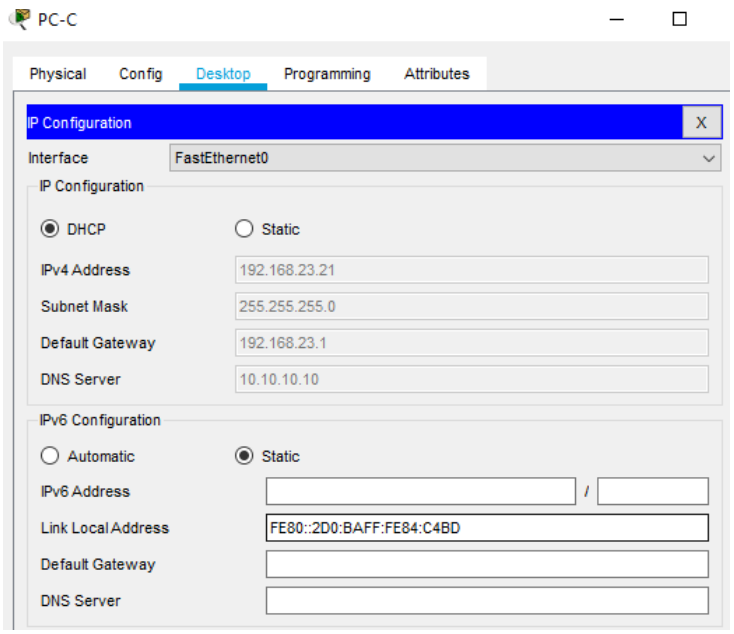

*Fuente: Autor*

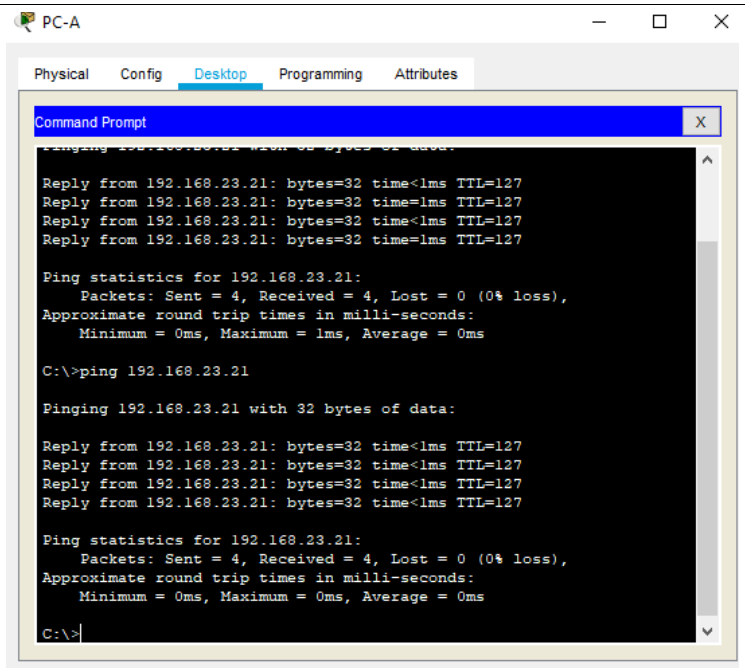
**Verificar el protocolo DHCP y la NAT estática**

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

*Tabla 27. Verificar el protocolo DHCP y la NAT estática*

| Prueba | Resultados |
|---|---|

| | |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP |  |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP |  |

| | |
|---|---|
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. |  |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | |

*Ping y configuraciones Ip*

**Configurar NTP**

*Tabla 28. Configurar la NTP*

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | R2#clock set 09:00:00 05 march 2016 |
| Configure R2 como un maestro NTP. | R2(config)#ntp master 5 |
| Configurar R1 como un cliente NTP. | R1(config)#ntp server 172.16.1.2 |
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1(config)#ntp update-calendar |
| Verifique la configuración de NTP en R1. | R1#show ntp |

*Se ajusta fecha y hora en R2 y se configura R2 como maestro NTP y R1 como cliente.*

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

**Restringir el acceso a las líneas VTY en el R2**

*Tabla 29. Restringir acceso a line VTY y 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 | R2(config)#ip access-list standard ADMIN-MGT<br>R2(config-std-nacl)#permit host 172.16.1.1 |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)#line vty 0 4<br>R2(config-line)#access-class ADMIN-MGT in |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#transport input telnet |
| Verificar que la ACL funcione como se espera | *R2 (config) show access-list* |

Se configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombres de línea VTY y permitir el acceso a telnet.

**Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

*Tabla 30. Comando CLI*

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | R2#show ip access-lists |
| Restablecer los contadores de una lista de acceso | R2#clear access-list counters ip |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | R2#show ip interface |

| | |
|---|---|
| ¿Con qué comando se muestran las traducciones NAT? | R2#show ip nat translations |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip nat translation |

*Tabla de preguntas y/o aclaración de dudas*

## CONCLUSIONES

- Gracias al desarrollo de este taller hemos logrado identificar cada uno de los dispositivos que intervienen en el proceso de configuración del sistema de redes y su implementación de acuerdo a los requisitos establecidos en la guía de actividades.
- Se logro la configuración de la topología sugerida en la prueba de habilidades, aplicando el conocimiento y habilidades obtenidas en el transcurso del diplomado de profundización.

## BIBLIOGRAFIA

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoW

## ANEXO 1. Enlace de descarga de archivos de simulación.

https://1drv.ms/u/s!AuTGKiJNBv9Zgybz4nQjN8gagA8U?e=3O6VR1

## ANEXO 2 Artículo Científico IEEE

https://1drv.ms/u/s!AuTGKiJNBv9ZgyyUrxwbBfCOMKhY?e=8GoTOw

# Escenario 2 Bajo la tecnología CISCO.

*Michael David Guerra Lizarazo*
*Universidad Nacional Abierta y a Distancia UNAD.*
*mdguerrali.unadvirtual.edu.co*

**Resumen**

Este diplomado se realiza para culminar la profundización de cisco, las practicas se desarrollaron en packet tracert que nos permitió crear los escenarios, los cuales nos pueden ayudar en nuestro entorno laboral aplicando estos conocimientos.

Este ejercicio tiene como objetivo solucionar el escenario 2 seleccionado, se documentará cada paso de la configuración de los dispositivos del escenario de las redes, al final se verificará la conectividad por medio de comandos, se manejarán la conectividad de los equipos configurándolos con dirección ip e ipv6, con protocolos de enrutamiento dinámico, configuración ssh o telnet, configuración de DHCP y NAT, se configura NTP, se verifica la conectividad para dar solución a los ejercicios.

**Palabras clave:** CCNA, CISCO, Conmutación, Electrónica, Enrutamiento, Redes.

**Abstract:**

This diploma is made to culminate the deepening of cisco, the practices were developed in packet tracert that allowed us to create the scenarios, which can help us in our work environment by applying this knowledge.

This exercise aims to solve the selected scenario 2, each step of the configuration of the devices in the network scenario will be documented, at the end the connectivity will be verified through commands, the connectivity of the equipment will be handled by configuring it with ip and ipv6 address, with dynamic routing protocols, ssh or telnet configuration, DHCP and NAT configuration, NTP configuration, the connectivity will be verified to give solution to the exercises.

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

**El tipo de letra de las cuatro secciones anteriores es Times New Roman de 10 puntos y negrilla. Solamente los títulos de cada sección van en itálica.**

## I. Introducción

Vivimos en un mundo donde todos los negocios no tienen los conocimientos suficientes para manejar las redes, por ese motivo es importante enseñarles las habilidades necesarias para que conozcan y adquieran conocimientos de cómo se configura el sistema de redes, logrando así una conectividad optima en las empresas.

Mostraremos los conocimientos que un administrador en redes debe tener para cumplir los lineamientos de las topologías de red, mediante configuración e instalación, por lo tanto, se mejorarán las habilidades al mostrar la configuración de estos dos escenarios, mostrando los comandos más utilizados e importantes en el momento de realizar dicha actividad.

En el escenario 2 se configurará una red pequeña donde se deberá configurar routers switch y equipos de cómputo que permitan y admitan conectividad ipv4 e ipv6 y sean seguros, con protocolos DHCP y protocolo en red NTP.

***Inicializar dispositivos***

**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.
Tabla 1. Inicializar y cargar todos los switch

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Router#erase startup-config |
| Volver a cargar todos los routers | Router#reload |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Switch#erase startup-config<br>Switch#delete vlan.dat |
| Volver a cargar ambos switches | **Switch#reload** |
| Verificar que la base | Switch>enable |

| | |
|---|---|
| de datos de VLAN no esté en la memoria flash en ambos switches | Switch#show flash |

En esta tabla se elimina toda la configuración del dispositivo, luego se reinicia el dispositivo, para eliminar la base de datos de VLAN y asi cargar los switch posteriormente detallamos que no esten en memoria flash

Configurar los parámetros básicos de los dispositivos
Configurar la computadora de Internet
Tabla 2. *Configurar la computadora de 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 1. Direccion Ip de servidor de internet.

Autor: Fuente

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

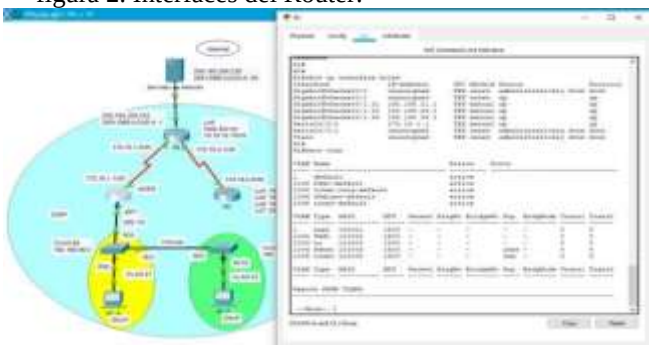
Configurar R1
Las tareas de configuración para R1 incluyen las siguientes
Tabla 3. Configurar R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | *Router(config)#no ip domain-lookup* |
| Nombre del router | Router(config)#hostname R1 |
| Contraseña de exec privilegiado cifrada | R1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | R1(config)#line console 0<br>R1(config-line)#password ciscoconpass R1(config-line)#login |
| Contraseña de acceso Telnet | R1(config-line)#line vty 0 4<br>R1(config-line)#password ciscoconpass R1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption |
| Mensaje MOTD | R1(config)#banner motd $Se prohibe el acceso no autorizado.$ |
| Interfaz S0/0/0 | Interfaz S0/0/0<br>R1(config)#interface serial 0/0/0<br>R1(config-if)#description Connection to R2<br>R1(config-if)#ip address 172.16.1.1<br>255.255.255.252<br>R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64<br>R1(config-if)#clock rate 128000<br>R1(config-if)#no shutdown |
| Rutas predeterminadas | R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0<br>R1(config)#ipv6 route ::/0 s0/0/0 |

**Nota:** Todavía no configure G0/1, ya mencionado se desactiva la búsqueda DNS, se configura el nombre como R1, agregamos contraseñas para EXEC privilegiado y acceso a consola y una vez hecho se encriptan por seguridad. Se establece la dirección ipv4 e ipv6 (consulte tabla 11) y frecuencia de reloj en 128000, con rutas predeterminadas establecidas en la tabla 11.

.

figura 2. Interfaces del Router.



Fuente: Autor

**Configurar R2**

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configurar R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R2 |
| Contraseña de exec privilegiado cifrada | R2(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | R2(config)#line console 0<br>R2(config-line)#password ciscoconpass<br>R2(config-line)#login |
| Contraseña de acceso Telnet | R2(config-line)#line vty 0 4<br>R2(config-line)#password ciscoconpass<br>R2(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R2(config-line)#service password- encryption |
| Habilitar el servidor HTTP | R2(config)#ip http server |
| Mensaje MOTD | R2(config)#banner motd $Se prohibe el acceso no autorizado.$ |
| Interfaz S0/0/0 | R2(config)#interface serial 0/0/0<br>R2(config-if)#description Connection to R1<br>R2(config-if)#ip address 172.16.1.2<br>255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64<br>R2(config-if)#no shutdown |
| Interfaz S0/0/1 | R2(config)#interface serial 0/0/1<br>R2(config-if)#description Connection to R3<br>R2(config-if)#ip address 172.16.2.2<br>255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64<br>R2(config-if)#clock rate 128000 R2(config-if)#no shutdown |
| Interfaz G0/0 (simulación de Internet) | R2(config)#interface gigabitEthernet 0/0<br>R2(config-if)#description Connection to Internet<br>R2(config-if)#ip address 209.165.200.233<br>255.255.255.248<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64<br>R2(config-if)#no shutdown |
| Interfaz loopback 0 (servidor web simulado) | R2(config-if)#Interface Loopback0 R2(config-if)#ip address 10.10.10.10<br>255.255.255.255 |
| Ruta predeterminada | R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0<br>R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 |

En esta tabla de configuraciones de R2 se desactiva la busqueda de DNS, se cambia nombre del router 2 a R2, establecemos contraseñas para el EXEC privilegiado y modo consola y a su vez encriptadas, contraseña a telnet para acceder a interfaz virtual, habilitamos http para pruebas de internet, una vez luego modificando interfaz s0/0/0, 0/0/1, G0/0 que es la simulada de internet y lookback que sera el servidor web simulado

Figura 3. Interfaces R2

Fuente: Autor

**Configurar R3**

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configurar R3

| Elemento o tarea de configuración | Especificación |
|---|---|

| | |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | R3<br>Router(config)#hostname R3 |
| Contraseña de exec privilegiado cifrada | R3(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | R3(config)#line console 0<br>R3(config-line)#password ciscoconpass<br>R3(config-line)#login |
| Contraseña de acceso Telnet | R3(config-line)#line vty 0 4<br>R3(config-line)#password ciscoconpass<br>R3(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | ***R3(config-line)#service password-encryption*** |
| Mensaje MOTD | R3(config)#banner motd $Se prohibe el acceso no autorizado.$ |
| Interfaz S0/0/1 | R3(config)#interface serial 0/0/1<br>R3(config-if)#description Connection to R2<br>R3(config-if)#ip address 172.16.2.1<br>255.255.255.252<br>R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64<br>R3(config-if)#no shutdown |
| Interfaz loopback 4 | R3(config-if)#Interface Loopback4 R3(config-if)#ip address 192.168.4.1<br>255.255.255.0 |
| Interfaz loopback 5 | R3(config-if)#Interface Loopback5 R3(config-if)#ip address 192.168.5.1<br>255.255.255.0 |
| Interfaz loopback 6 | R3(config-if)#Interface Loopback6 R3(config-if)#ip address 192.168.6.1<br>255.255.255.0 |
| Interfaz loopback 7 | R3(config-if)#Interface Loopback7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64<br>*no ip address*<br>*ipv6 address* |
| | ***2001:DB8:ACAD:3::1/64*** |
| Ruta predeterminada | R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1<br>R3(config)#ipv6 route ::/0 serial 0/0/1 |

Tabla R3 se desactiva búsqueda DNS, nombre del router 3 pasa a ser R3 con su clave a EXEC privilegiado, a consola y telnet, una vez estas cifradas e encriptadas son su respectivo mensaje en lugar de error de acceso al loguearse; se establece la dirección ipv4 e ipv6 para activar interfazes s0/0/1 y interfaz subred como Interfaz loopback 4, Interfaz loopback 5, Interfaz loopback 6, Interfaz loopback 7, con sus ruta predeterminadas.

*Configurar S1*

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configurar S1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | *Switch(config)#no ip domain-lookup* |
| Nombre del switch | Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | S1(config)#enable secret ciscoenpass |
| Contraseña de acceso a la consola | S1(config)#line console 0<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login |
| Contraseña de acceso Telnet | S1(config-line)#line vty 0 4<br>S1(config-line)#password ciscoconpass<br>S1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | *S1(config-line)#service password- encryption* |
| Mensaje MOTD | S1(config)#banner motd $Se prohibe el acceso no autorizado.$ |

Tabla de S1 se tiene en cuenta la desactivación de la busqueda DNS, se reescribe su nombre a S1, se anexan claves para el modo EXEC privilegiado, consola y acceso

a telnet con su respectivo mensaje por si llega haber errores de logueo, y encriptadas por seguridad.

*Verificar la conectividad de la red*

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

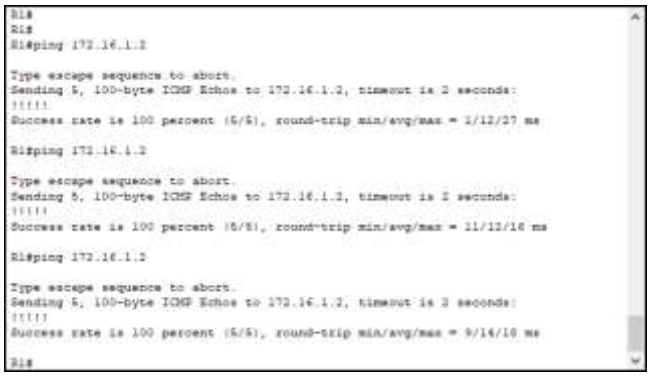
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

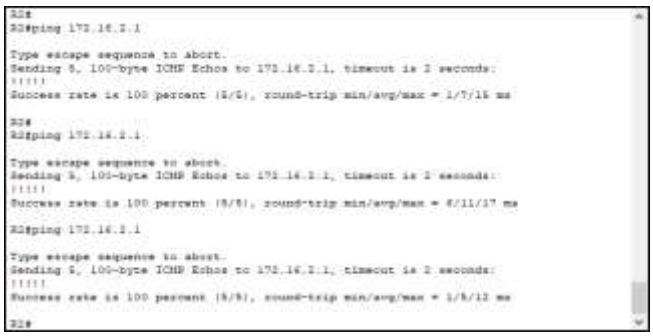
Tabla 7. Configurar conectividad de la red.

| **Dede** | **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.

Figura 4. Ping




Fuente: Autor

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

**Configurar S1**

La configuración del S1 incluye las siguientes tareas:

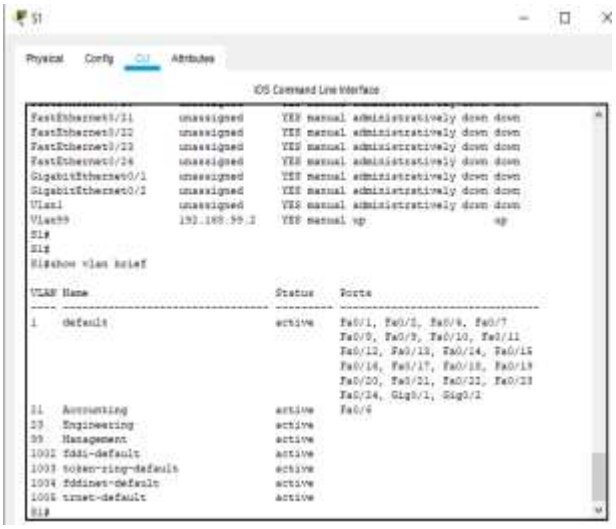
Tabla 8. Configurar S1-VLAN

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | S1(config)#vlan 21<br>S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23<br>S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99<br>S1(config-vlan)#name Administracion |
| Asignar la dirección IP de administración. | S1(config)#interface vlan 99<br>S1(config-if)#ip address 192.168.99.2<br>255.255.255.0<br>S1(config-if)#no shutdown |
| Asignar el gateway predeterminado | S1(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Forzar el enlace troncal en la interfaz F0/5 | S1(config-if)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S1(config-if)#interface range f0/1-2, f0/4, f0/6- 24, g0/1-2<br>S1(config-if-range)#switchport mode access |
| Asignar F0/6 a la VLAN 21 | S1(config-if-range)#interface fastEthernet 0/6 |

| | |
|---|---|
| | S1(config-if)#switchport access vlan 21 |
| Apagar todos los puertos sin usar | S1(config-if)#interface range f0/1-2, f0/4, f0/7- 24, g0/1-2<br>S1(config-if-range)#shutdown |

Se crean las bases de datos contabilidad, ingeniería y administración, se asigna direcciones ipv4 a la vlan de administración y usamos la IP asignada al S1 en el diagrama de topología, se asignan el Gateway predeterminado y se fuerzan troncales F/03, F/05, se configuran el resto de puertos como puertos de acceso y apagamos los sin usar por seguridad.

Figura 5. Configuración CLI S1




Fuente: Autor.

*Configurar el S3*

La configuración del S3 incluye las siguientes tareas:

Tabla 9. Configurar S3-VLAN

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | S3(config)#vlan 21<br>S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23<br>S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99<br>S3(config-vlan)#name Administracion |
| Asignar la dirección IP de administración | S3(config-vlan)#interface vlan 99<br>S3(config-if)#ip address 192.168.99.3<br>255.255.255.0<br>S3(config-if)#no shutdown |
| Asignar el gateway predeterminado. | S3(config)#ip default-gateway 192.168.99.1 |
| Forzar el enlace troncal en la interfaz F0/3 | S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S3(config)#interface range f0/1-2, f0/4-24, g0/1-2<br>S3(config-if-range)#switchport mode access |
| Asignar F0/18 a la VLAN 23 | S3(config-if-range)#interface fastEthernet 0/18<br>S3(config-if)#switchport access vlan 23 |
| Apagar todos los puertos sin usar | S3(config-if)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2<br>S3(config-if-range)#shutdown |

*Se crean las bases de datos contabilidad, ingeniería y administración, se asigna direcciones ipv4 a la vlan de administración y usamos la* IP asignada al S1 en el diagrama de topología, se asignan el Gateway predeterminado y se fuerzan troncales F/03, F/05, se configuran el resto de puertos como puertos de acceso y apagamos los sin usar por seguridad y por último se asigna F0/18 a la VLAN 23

*Configurar R1*

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Configurar R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description LAN de Contabilidad |

| | |
|---|---|
| | R1(config-subif)#encapsulation dot1Q 21<br>R1(config-subif)#ip address 192.168.21.1<br>255.255.255.0 |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | R1(config-subif)#interface gigabitEthernet 0/1.23<br>R1(config-subif)#description LAN de Ingenieria<br>R1(config-subif)#encapsulation dot1Q 23<br>R1(config-subif)#ip address 192.168.23.1<br>255.255.255.0 |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | R1(config-subif)#interface gigabitEthernet 0/1.99<br>R1(config-subif)#description LAN de Administracion<br>R1(config-subif)#encapsulation dot1Q 99<br>R1(config-subif)#ip address 192.168.99.1<br>255.255.255.0 |
| Activar la interfaz G0/1 | R1(config-subif)#int g0/1<br>R1(config-if)#no shutdown |

Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz, Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz, Descripción: LAN de Administración Asignar la VLAN 99

Asignar la primera dirección disponible a esta interfaz

*Verificar la conectividad de la red*

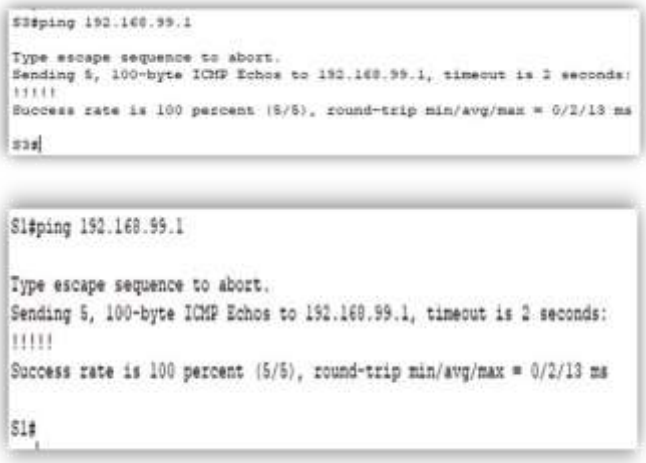
Utilice el comando ping para probar la conectividad entre los switches y el R1.

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:

Tabla 11. Verificar la red.

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

Figura 6. Ping comprobando conectividad




Fuente: Autor

*Configurar el protocolo de routing dinámico OSPF*

*Configurar OSPF en el R1*

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 12. Configurar OSPF en el R1

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)#router ospf<br>R2(config-router)#version 3 |
| Anunciar las redes conectadas directamente | R1(config-router)#do show ip route |

| | |
|---|---|
| | connected<br>C 172.16.1.0/30 is directly<br>connected, Serial0/0/0<br>C 192.168.21.0/24 is directly<br>connected, GigabitEthernet0/1.21<br>C 192.168.23.0/24 is directly<br>connected, GigabitEthernet0/1.23<br>C 192.168.99.0/24 is directly<br>connected, GigabitEthernet0/1.99<br>R1(config-router)#network 172.16.1.0<br>R1(config-router)#network 192.168.21.0<br>R1(config-router)#network 192.168.23.0<br>R1(config-router)#network 192.168.99.0 |
| Establecer todas las interfaces LAN como pasivas | R1(config-router)#passive-interface gigabitEthernet 0/1.21<br>R1(config-router)#passive-interface gigabitEthernet 0/1.23<br>R1(config-router)#passive-interface gigabitEthernet 0/1.99 |
| Desactive la sumarización automática | R1(config-router)#no auto-summary |

Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 18) y establecemos interfaces LAN como pasivas.

Figura 7. Red protocolo OSPF en R1

Fuente: Autor

**Configurar OSPF en el R2**

La configuración del R2 incluye las siguientes tareas:

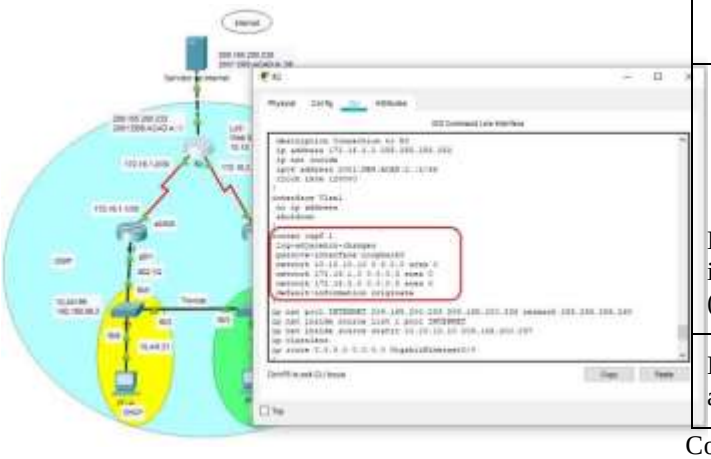
Tabla 13. Configurar OSPF en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar OSPF área 0 | R2(config)#router osfp<br>R2(config-router)#version 3 |
| Anunciar las redes conectadas directamente | R2(config-router)#do show ip<br>route connected<br>C 10.10.10.10/32 is directly<br>connected, Loopback0<br>C 172.16.1.0/30 is directly<br>connected, Serial0/0/0<br>C 172.16.2.0/30 is directly<br>connected, Serial0/0/1<br>C 209.165.200.232/29 is<br>directly connected,<br>GigabitEthernet0/0<br>R2(config-router)#network 10.10.10.10<br>R2(config-router)#network 172.16.1.0<br>R2(config-router)#network 172.16.2.0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config-router)#passive-interface loopback 0 |
| Desactive la sumarización | R2(config-router)#no auto- |

| | |
|---|---|
| automática. | summary |

Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 19) y establecemos interfaces LAN como pasivas.

Figura 8. Red protocolo OSPF en R2

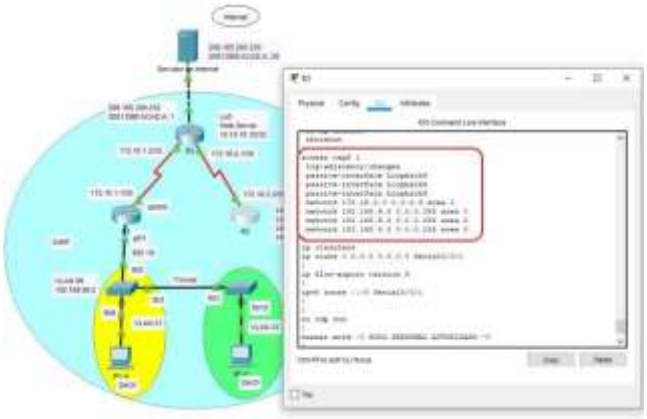


Fuente: Autor

| | |
|---|---|
| | 172.16.2.0<br>R2(config-router)#network<br>192.168.4.0<br>R2(config-router)#network<br>192.168.5.0<br>R2(config-router)#network<br>192.168.6.0 |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R2(config-router)#passive-interface loopback 4<br>R2(config-router)#passive-interface loopback 5<br>R2(config-router)#passive-interface loopback 6 |
| Desactive la sumarización automática. | R2(config-router)#no auto-summary |

Configuramos OSPF y anunciamos redes conectadas directamente (observe figura 20) y establecemos interfaces LAN como pasivas

Figura 9. Red protocolo OSPF en R3



Fuente: Autor

**Configurar OSPFv3 en el R3**

La configuración del R3 incluye las siguientes tareas:

Tabla 14. Configurar OSPF en el R3

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar OSPF área 0 | ***R2(config)# ipv6 router ospf 1 R3(config-rtr)# router-id 3.3.3.3*** |
| Anunciar redes IPv4 conectadas directamente | R2(config-router)#do show ip<br>route connected<br>C 172.16.2.0/30 is directly<br>connected, Serial0/0/1<br>C 192.168.4.0/24 is directly<br>connected, Loopback4<br>C 192.168.5.0/24 is directly<br>connected, Loopback5<br>C 192.168.6.0/24 is directly<br>connected, Loopback6<br>R2(config-router)#network |

*Verificar la información de OSPF*

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

Tabla 15. Verificar informacion de OSPF

| **Pregunta** | Respuesta |
|---|---|
| R2#show ip route ospf | R2#show ip protocols |

| | |
|---|---|
| ¿Qué comando muestra solo las rutas OSPF? | R2#show ip route ospf |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | R2#show run \| section router ospf<br>router ospf |

Tabla de preguntas y/o aclaración de dudas

**Implementar DHCP y NAT para IPv4**

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

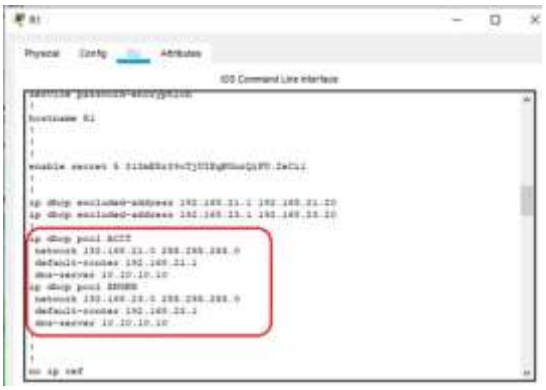
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Implementar DHCP y NAT para Ipv4

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 |
| Crear un pool de DHCP para la VLAN 21. | R1(config)#ip dhcp pool ACCT<br>R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#default-router 192.168.21.1 |
| Crear un pool de DHCP para la VLAN 23 | R1(dhcp-config)#ip dhcp pool ENGNR<br>R1(dhcp-config)#network 192.168.23.0 255.255.255.0<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#default-router 192.168.23.1 |

*Reservamos las primeras 20 direcciones ip en la VLAN 21 para configuraciones estáticas* Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas, se crea un pool de DHCP para la VLAN 21. Y por ultimo Crear un pool de DHCP para la VLAN 23

Figura 9. Configuración dinámica de servidor



Fuente: Autor

*Configurar la NAT estática y dinámica en el R2*

La configuración del R2 incluye las siguientes tareas:

Tabla 17. Configurar la nat estatica y dinamica en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | R2(config)#username webuser privilege 15 secret cisco12345 |
| Habilitar el servicio del servidor HTTP | R2(config)#ip http server |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | R2(config)#ip http authentication local |
| Crear una NAT estática al servidor web. | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 |
| Asignar la interfaz interna y externa para la | R2(config)#ip nat inside source static 10.10.10.10 |

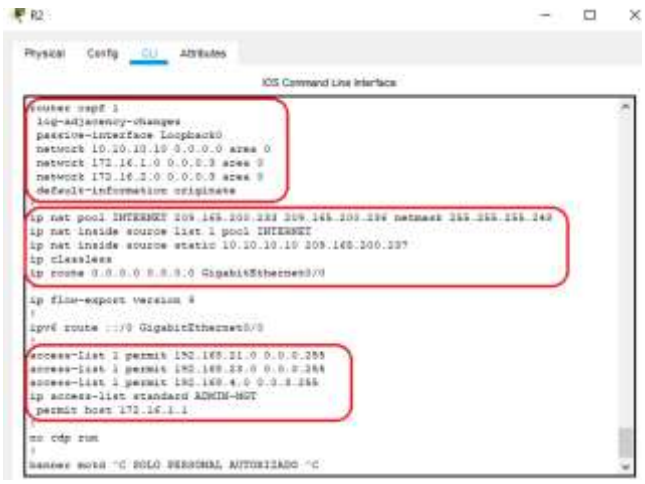
| | |
|---|---|
| NAT estática | 209.165.200.229 |
| Configurar la NAT dinámica dentro de una ACL privada | R2(config)#access-list 1 permit<br>192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit<br>192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.4.0<br>0.0.3.255 |
| Defina el pool de direcciones IP públicas utilizables. | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3<br>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask<br>255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

*Se* crea una base de datos local con una cuenta de usuario, se habilita el servicio de servidor http se configura para autenticar, una vez hecho se crea la NAT estatica a dicho servidor web se le asigan interfaces internas y externas 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

Figura 11. Configuración R2

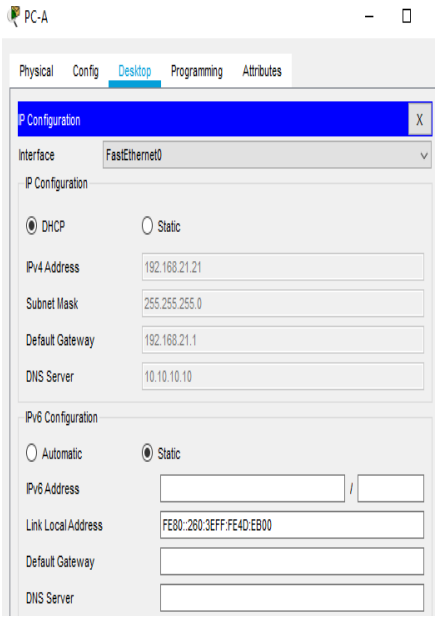
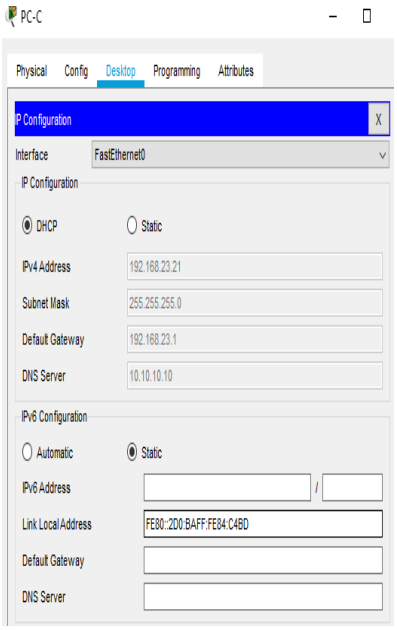


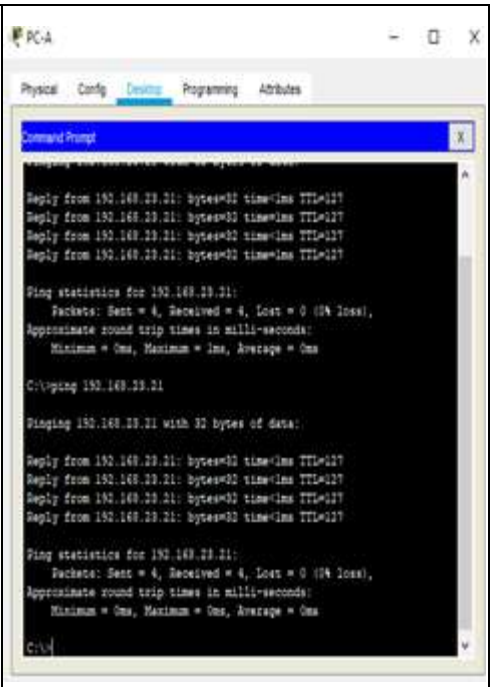

Fuente: Autor

Verificar el protocolo DHCP y NAT estatica

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

Tabla 18. *Verificar el protocolo DHCP y la NAT estática*

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

| | |
|---|---|
| Verificar que la PC-A pueda hacer ping a la PC-C<br><br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC |  |
| Utilizar navegador web la computadora Internet pa acceder servidor w (209.165.200.22 Iniciar sesión c el nombre usuario **webus** y la contraseña | Input telnet |
| Verificar que ACL funcio como se espera | R2(config)#show access-list |

Ping y configuraciones Ip

**Configurar NTP**

**Tabla. 19.** Configurar la NTP

| **Elemento o tarea de configuración** | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | R2#clock set 09:00:00 05 march 2016 |
| Configure R2 como un maestro NTP. | R2(config)#ntp master 55 |
| Configurar R1 como un cliente NTP. | R1(config)#ntp server 172.16.1.2 |

| | |
|---|---|
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | R1#show ntp |

Se ajusta fecha y hora en R2 y se configura R2 como maestro NTP y R1 como cliente.

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

*Restringir el acceso a las líneas VTY en el R2*

Tabla 20. Restringir acceso a line VTY y 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 | R2(config)#ip access-list standard ADMIN-MGT<br>R2(config-std-nacl)#permit host 172.16.1.1 |
| Aplicar la ACL con nombre a las líneas VTY | R2(config)#line vty 0 4<br>R2(config-line)#access-class ADMIN-MGT in |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-line)#transport input telnet |
| Verificar que la ACL funcione como se espera | R2 (config) show access-list |

**Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

Tabla 21. Comando CLI

| **Descripción del comando** | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | R2#show ip access-lists |
| Restablecer los contadores de una lista de acceso | R2#clear access-list counters ip |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | R2#show ip interface |
| ¿Con qué comando se muestran las traducciones NAT? | R2#show ip nat translations |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip nat translation |

Se configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2, se aplica la ACL con nombres de línea VTY y permitir el acceso a telnet.

## CONCLUSIONES

El trabajo realizado durante el diplomado ayudo a resolver este escenario y como la configuración de redes puede ayudar a una empresa a mejorar sus condiciones.

Con el desarrollo fue posible demostrar destrezas en cuanto a la configuración de equipos de red Cisco, como Routers y Switches. Se logró llevar a cabo de manera exitosa protocolos de enrutamiento dinámico como OSPF y otros servicios como DHCP, listas de acceso, Nat y aseguramiento de dispositivos Cisco.

Finamente, aplicar comandos para verificar funcionalidad y resolver problemas presentados con las funcionalidades previamente mencionadas.

## REFERENCIA


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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei- NT1IlnMfy2rhPZHwEoW

Bitacora Byte. (18 de julio de 2017). Configurar DHCP en router CISCO. Recuperado el 18 de octubre de 2020, de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado el 18 de octubre de 2020 de: https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#8

Cisco. (10 de agosto de 2005). Configuración de una puerta de enlace de último recurso mediante comandos IP. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocolrip/16448-default.html

Cisco. (sf de sf de 2020). Guía de configuración del software del switch Catalyst 3750-X y 3560-X, versión 12.2 (55) SE. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software /release/12-2_55_se/configuration/guide/3750xscg/swsdm.html

Cisco. (21 de noviembre de 2007). Información sobre los modos de loopback en routers de Cisco. Recuperado el 18 de Octubre de 2020, de Cisco: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-modeatm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337- atmloopback.htm

## BIOGRAFIA.

**Michael David Guerra Lizarazo** nacido en Valledupar- Cesar en el año 1997 Tecnólogo en análisis y desarrollo de sistemas ADSI SENA. Ha trabajado en la area de desarrollo y actualización de bases de datos, empresas como Clinica Valledupar y Clinica Arenas, analista de sistemas en transporte terrestre, empresa Copetran ltda. Como aspirante al título de ingeniero de sistemas se llevó a cabo este artículo con el fin de dar respuesta al escenario 2 por medio de la tecnología CISCO.