SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGIAS CISCO

DEYANIRA POLO ANAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *DE SISTEMAS*
LA PLATA HUILA
2021

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO USO DE TECNOLOGIAS CISCO

DEYANIRA POLO ANAYA

Diplomado de opción de grado presentado para optar el título de INGENIERA DE SISTEMAS

DIRECTORA:
NANCY AMPARO GUACA GIRON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE *SISTEMAS*
LA PLATA HUILA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

La Plata Huila, 02 de diciembre de 2021

AGRADECIMIENTOS

A cada uno de los tutores que han hecho parte de mi formación profesional, ya que cada uno de ellos ha aportado un granito de arena en que ame mi profesión y que desee adquirir los mejores conocimientos para ponerlos al servicio de quienes lo necesiten.

DEDICATORIA

Este trabajo está dedicado a Dios por su infinita misericordia y amor por regalarnos el don de la vida y llenarnos cada día con su amor incondicional, a mi familia y en especial a mi madre y a mi hijo quienes han sido mi motor y mi sostén para alcanzar mis sueños de ser una profesional, quienes con su apoyo y con mi esfuerzo he podido gradualmente ir alcanzando peldaños para lograr este sueño y ser una gran Ingeniera de Sistemas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Dhcp: (Dynamic Host Configuration Protocol) Es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red

Dirección Ip: Hace referencia a un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

Dirección Ipv6: Corresponde a la versión 6 del Protocolo de Internet (Internet Protocol), es decir, es la sexta versión del protocolo que hace posible conectar dispositivos en Internet, identificándolos con una dirección unívoca

Enrutamiento: Proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

Loopback: Hace referencia a una interfaz de red virtual. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

Mascara de Subred: Combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

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

RESUMEN

En el contenido del presente documento, encontramos topología, requerimientos y solución a dos escenarios aplicados en el simulador Packet Tracer, donde se brinda una configuración a cada uno de los dispositivos como Switches, Routers, y pcs, además de servidores de internet, aplicando configuración IPV4 e IPV6 y permitiendo conexiones para cada uno de los elementos conectados a la red, se realizan las configuraciones del IPv4 y del IPv6 en el dispositivo del punto de acceso de las redes y se hace el diagnóstico con el comando ping, para verificar el estado de determinada conexión de host local.

Palabras claves: CISCO, CCNA, Conmutación, Enrutamiento, Redes

ABSTRACT

In the content of this document, we find topology, requirements and solution to two scenarios applied in the Packet Tracer simulator, where a configuration is provided to each of the devices such as Switches, Routers, and PCs, as well as internet servers, applying configuration IPV4 and IPV6 and allowing connections for each of the elements connected to the network, the IPv4 and IPv6 configurations are made in the network access point device and the diagnosis is made with the ping command, to verify the status of certain local host connection.

Keywords: CISCO, CCNA, Switching, Routing, Networking.

.

INTRODUCCIÓN

Teniendo como base los grandes avances generados en la comunicación y de acuerdo a las nuevas necesidades requeridas en temas de información, para que se transfiera de forma segura y de calidad, es de vital importancia hacer un buen uso de la tecnología, y las redes nos permiten la posibilidad de conectarnos ofreciendo mejores servicios a beneficio de una comunidad en particular, a fin de estimular y ofrecer mejores oportunidades para el desarrollo social.

Mediante el presente informe se pretende aplicar conocimientos de configuración de las IP usando diferentes máscaras de subred y haciendo las configuraciones respectivas dando conectividad a la red.

En el presente documento se hallan dos escenarios afines con redes y el objetivo es aplicar cada uno de los conceptos obtenidos en el diplomado de cisco para la apropiada configuración de los dispositivos y de esta manera obtener el establecimiento de una conexión efectiva.

REQUERIMIENTOS ESCENARIO

ESCENARIO No. 1

Figura 1. Topología Unad. Escenario No. 1

Fuente: 1 UNAD

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

Objetivos

Parte 1: Construir en el simulador la Red

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

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

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

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

Aspectos básicos/situación

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

Parte 1: Construya la Red

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

DESARROLLO ESCENARIO 1

Figura 2. Topología Creada Escenario No. 1

Fuente: 2 Propia.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.
Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1- Direccionamiento IP

ITEM	REQUERIMIENTO
Dirección de Red	192.168.X.0 Donde se le asigne al octeto donde se encuentra la X los dos últimos dígitos de mi cedula de ciudadanía la cual termina en 47 Quedando así 192.168.47.0 con prefijo 24 por defecto
Requerimiento de Host Subred LAN 1	100
Requerimiento de Host Subred LAN 2	50
R1 G0/0/0	192.168.47.129/26
R1 G0/0/1	192.168.47.1/25
S1 SVI	192.168.47.2/25
PC-A	192.168.47.126/25
PC-B	192.168.47.190/26

Fuente 1. Propia

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2 Configuración R1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda de DNS	Se aplica mediante el comando R1(config)#no ip domain-lookup
Nombre del Router	Se le asigno R1 mediante el comando Router(config)#hostname R1
Nombre de dominio	El nombre del dominio se asignó mediante el comando R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para modo EXEC privilegiado	Se asigno mediante el comando R1(config)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login
Contraseña de acceso a la consola	Se digita los comandos R1(config)#line vty 0 12 R1(config-line)#password ciscoenpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	Se establece mediante los comandos R1(config)#service password min-length 10
Crear un usuario administrativo en la base de datos local	Se designa mediante los siguientes comandos R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local R1(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura con los comandos R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	Se configura con los comandos R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	R1(config-line)#line console 0 R1(config-line)# service password encryption
Configure un MOTD Banner	R1(config)#banner motd "ACCESO RESTRINGIDO "SOLO PERSONAL AUTORIZADO""
Configurar interfaz G0/0/0	R1(config)#interface g0/0/0 R1(config-if)#ip address 192.168.47.129 255.255.255.192 R1(config-if)#description LAN1 R1(config-if)#no sh R1(config-if)#exit
Configurar interfaz G0/0/1	R1(config)#interface g0/0/1 R1(config-if)#ip address 192.168.47.1 255.255.255.128 R1(config-if)#no sh R1(config)#exit
Generar una clave de cifrado RSA	R1(config)#config t R1(config)#crypto key generate rsa general-keys modulus 1024 R1(config)#login local R1(config)#transport input ssh R1(config)#exit

Fuente 2. Propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Configuración S1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda de DNS	Se aplica mediante el comando R1(config)#no ip domain-lookup
Nombre del Router	Se le asigno S1 mediante el comando Router(config)#hostname S1
Nombre de dominio	El nombre del dominio se asignó mediante el comando S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para modo EXEC privilegiado	Se asigno mediante el comando S1(config)#line console 0 S1(config-line)#password ciscoenpass S1(config-line)#login
Contraseña de acceso a la consola	Se digita los comandos S1(config)#line vty 0 12 S1(config-line)#password ciscoenpass S1(config-line)#login S1(config-line)#exit

Crear un usuario administrativo en la base de datos local	Se designa mediante los siguientes comandos S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura con los comandos S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit
Configurar VTY solo aceptando SSH	Se configura con los comandos S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config-line)#line console 0 S1(config-line)# service password encryption
Configure un MOTD Banner	S1(config)#banner motd "ACCESO RESTRINGIDO "SOLO PERSONAL AUTORIZADO""
Configurar la interfaz de administración (SVI)	S1config t S1(config)#interface LAN 1 (config)#ip address 192.168.47.2 255.255.255.128 S1(config)#no sh S1(config)#end copy running-config startup-config R1(config-if)#exit
Configuración del gateway predeterminado	S1config t S1(config)#ip default-gateway 192.168.10.1
Generar una clave de cifrado RSA	R1(config)#config t R1(config)#crypto key generate rsa general-keys modulus 1024 R1(config)#line vty 0 4 R1(config)#login local R1(config)#transport input ssh R1(config)#exit

Fuente 3. Propia

Paso 2. Configurar los equipos

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

Tabla 4. Configuración PC-A

PC-A Network Configuration	
Descripción	LAN1
Descripción física	
Dirección IP	192.168.47.126/25
Mascara de subred	255.255.255.128
Gateway Predeterminado	192.168.10.1

Fuente 4. Propia

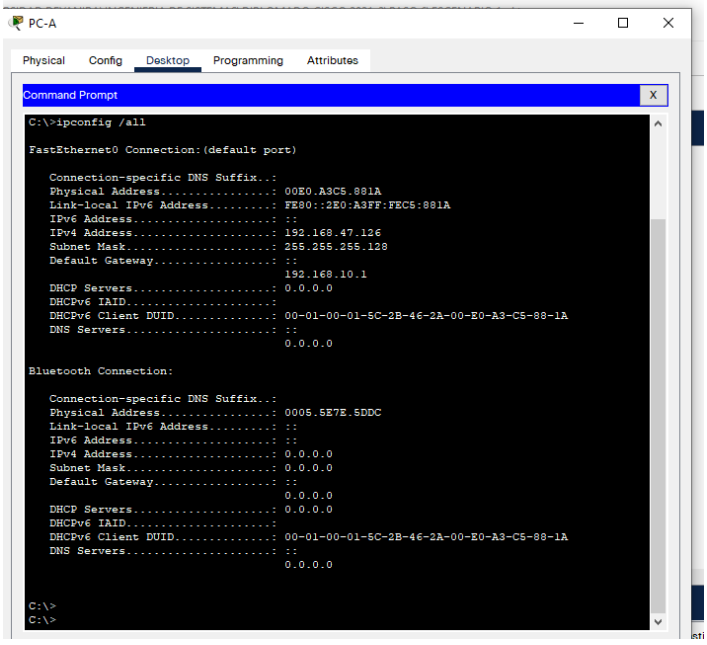
Tabla 5. Configuración PC-B

PC-B Network Configuration	
Descripción	LAN 2
Descripción física	
Dirección IP	192.168.47.190/26
Mascara de subred	255.255.255.192
Gateway Predeterminado	192.168.10.1

Fuente 5. Propia

Aplicación Comando ipconfig /all a la PC-A

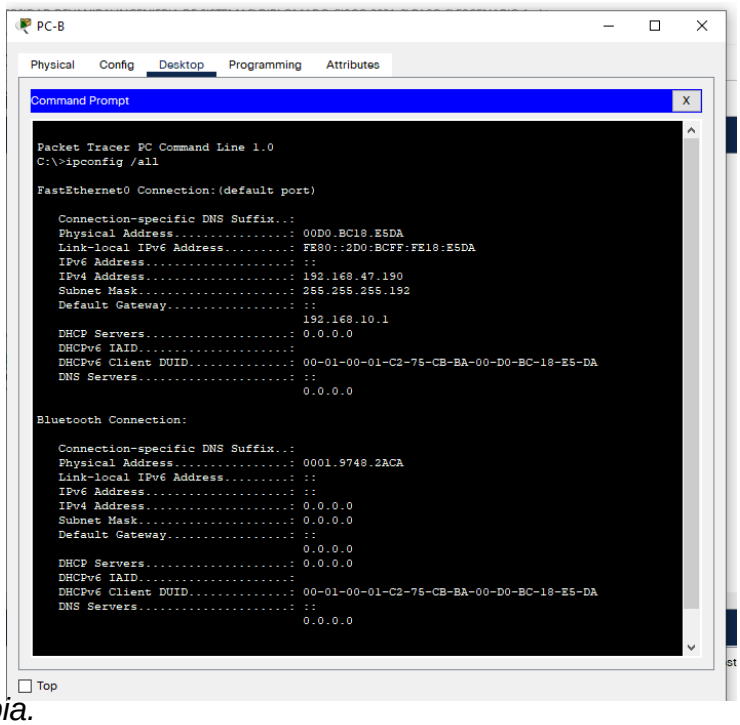
Figura 3. Comando Ipconfig /all PC-A



Fuente: 3. Propia

Aplicación Comando Ipconfig /all PC-B

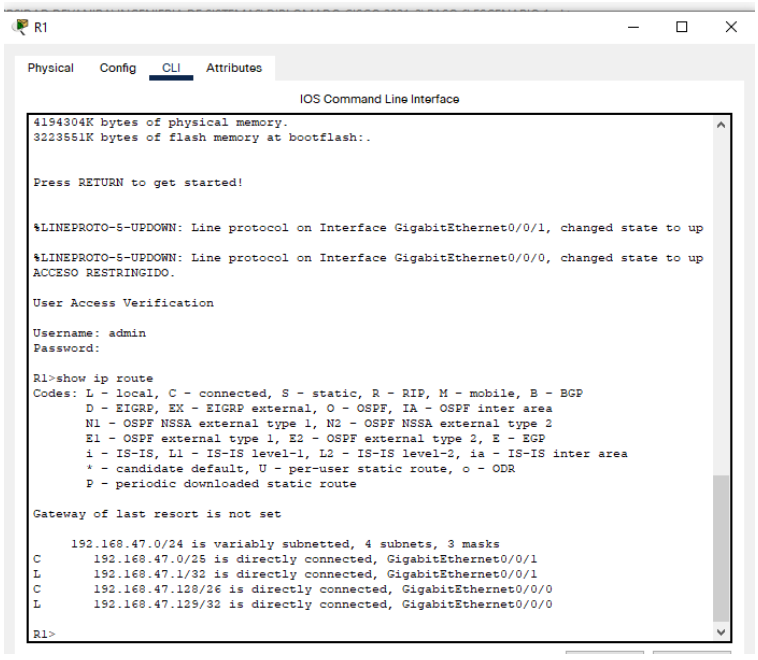
Figura 4. Comando Ipconfig /all PC-B



Fuente: 4. Propia.

Comando Show Ip Route

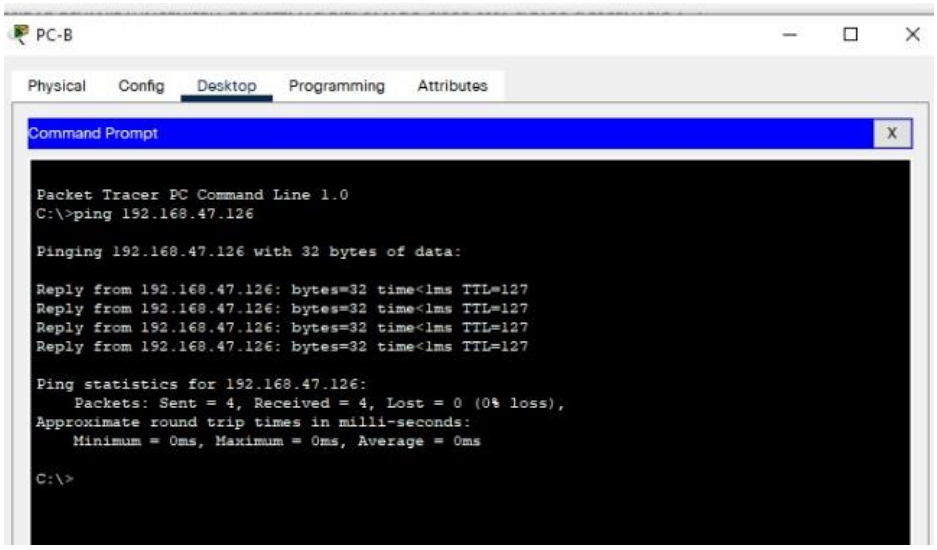
Figura 5. Comando Show IP Route



Fuente: 5. Propia.

Comando Ping

Figura 6.Ping PC



Fuente: 6. Propia.

ESCENARIO 2

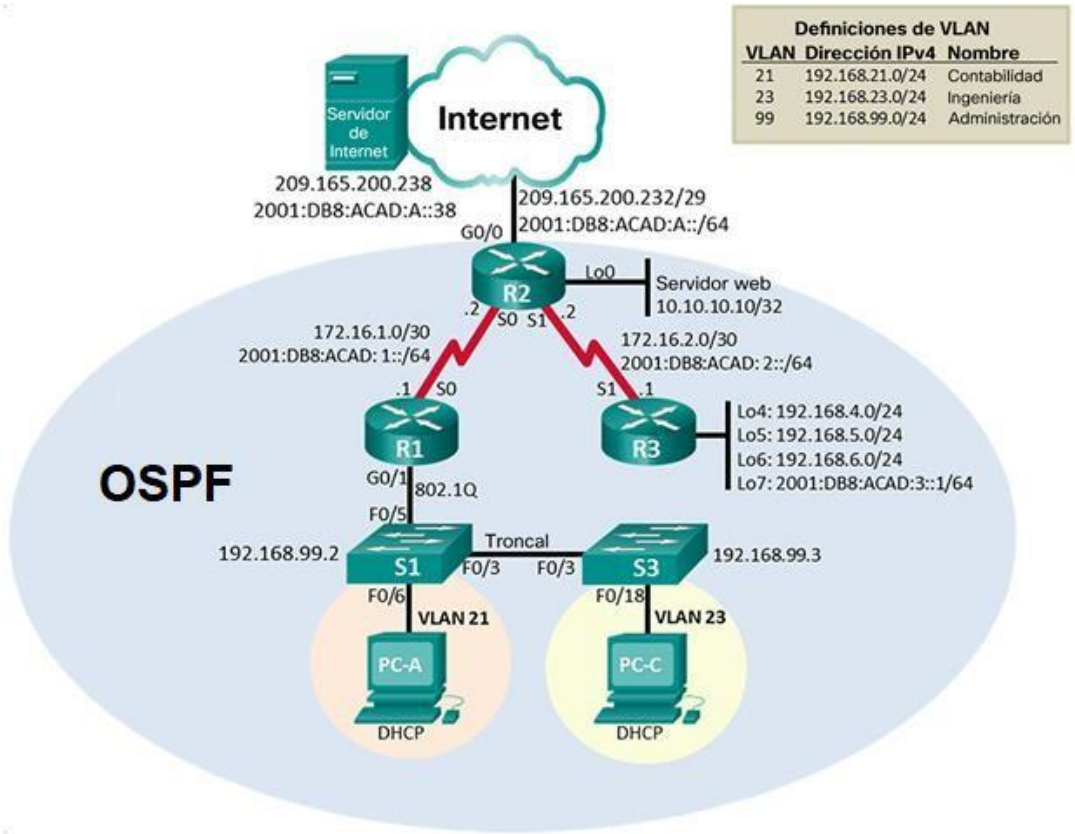
REQUERIMIENTOS ESCENARIO

Escenario:

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuraciónde 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 7. Topología UNAD



Fuente: 7. Unad

DESARROLLO ESCENARIO 2

Parte 1: Inicializar dispositivos

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

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

Para realizar la configuración es necesario que los dispositivos estén limpios y que se borren las configuraciones anteriores para que más adelante no se presenten errores. Por lo anterior se ejecuta el comando erase startup-config para la eliminación de la configuración de inicio y reload para para deshacer los últimos cambios realizados. En los switchs se eliminan las bases de datos de la Vlan anterior y con el comando Show flash se hace la verificación.

Tabla 6. Inicialización de Routers y Switches

Tarea	Comando de ios
Eliminar el archivo startup-config de todos los routers	En cada Router se dan los comandos Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload Se da inicialización Hardware de nuevo a los routers
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	En cada Switch se ejecutan los comandos Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload Se da inicialización Hardware de nuevo a los Switch
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#enable Switch#show flash

Fuente 6. Propia

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

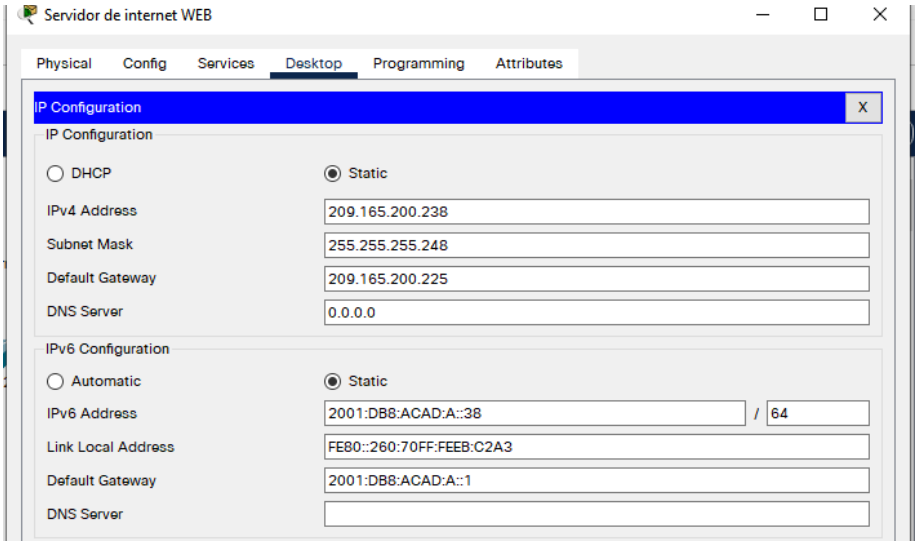
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología): IP, consulte la topología):

Tabla 7 Configuración de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	Gateway: 209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64 es la ipv6
Gateway predeterminado IPv6	Gateway: 2001:DB8:ACAD:A::1/64

Fuente 7. Propia

Figura 8. Configuración Servidor de Internet



Fuente: 8- Propia.

Paso 2: Configurar R1

Se requiere la configuración del router que proporcione conectividad a nivel de red con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que más adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y así proporcionar seguridad, se realiza la configuración de las interfaces del dispositivo.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1 Paso 2 Parte 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config T Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del Router	Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	Se aplica el comando R1(config)#enable secret class
Contraseña de acceso a la consola	Se aplican los comandos R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)# login R1(config-line)#
Contraseña de Acceso Telnet	Se aplican los comandos R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#
Cifrar las contraseñas de texto no cifrado	Se aplican los comandos R1(config)#line console 0 R1(config-line)#service password-encryption
Mensaje MOTD	Se ejecuta el comando R1(config)#banner motd "Se prohbe el acceso no autorizado"
Interfaz S0/2/0	Se ejecutan los comandos R1(config)#int s0/2/0 R1(config-if)#description interface hacia el router R2 R1(config-if)#exit R1(config)#ipv6 unicast-routing R1(config)#int s0/2/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64 R1(config-if)#clock rate 128000

	R1(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/2/0, changed state to down R1(config-if)#exit R1(config)#
Rutas Predeterminadas	Se ejecutan los comandos R1#enable R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#ipv6 route ::/0 s0/2/0 R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2 R1(config)#exit

Fuente 8. Propia

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9 Configuración R2 Paso 3 Parte 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecutan los comandos Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#
Nombre del Router	Se ejecutan los comandos Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Se ejecutan los comandos R2(config)#enable secret class
Contraseña de acceso a la consola	Se ejecutan los comandos R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de Acceso Telnet	Se ejecutan los comandos R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login

	R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Se ejecuta n los comandos R2(config)#service password-encryption
Habilitar el servidor HTTP	El comando http no sirve en ninguna version de los routers
Mensaje MOTD	Se ejecutan los comandos R2(config)#banner motd #se prohibe el acceso no autorizado# R2(config)#
Interfaz S0/0/0	Se ejecutan los comandos R2(config)#ipv6 unicast-routing R2(config)#int s0/2/0 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no sh R2(config-if)# %LINK-5-CHANGED: Interface Serial0/2/0, changed state to up R2(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up R2(config-if)#
Interfaz S0/0/1	Se ejecutan los comandos R2(config)#int s0/2/1 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh %LINK-5-CHANGED: Interface Serial0/2/1, changed state to down R2(config-if)# R2(config-if)#
Interfaz G0/0 (Simulación de Internet)	Se ejecuta los comandos R2(config-if)#int g0/0/0

	R2(config-if)#description interface hacia internet R2(config-if)#exit R2(config)#ipv6 unicast-routing R2(config)#int G0/0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 R2(config-if)#no sh R2(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up R2(config-if)#
Interfaz Loopback 0 (Servidor web simulado)	Se ejecutan R2(config-if)#int loopback 0 R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up description servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.252
Ruta predeterminada	Se ejecutan R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2(config)#ipv6 route ::/0 2001:db8:acad:1::1 R2(config)#ipv6 route ::/0 2001:db8:acad:2::1 R2(config)#exit R2#

	%SYS-5-CONFIG_I: Configured from console by console

Fuente 9. Propia

Paso 4: Configurar R3

Se realiza la configuración del router que provea conectividad a nivel de red en el modelo OSI con el fin de encauzar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que más adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y asi proporcionar seguridad, se realiza la configuración de las interfaces del dispositivo como la S0/0/1 y la loopback 4,5,6 y 7.

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecuta el comando Router(config)#no ip domain-lookup
Nombre del router	Se ejecuta el comando Router(config)#hostname R3 R3(config)#
Contraseña de exec privilegiado cifrada	Se ejecuta el comando R3(config)#enable secret class
Contraseña de acceso a la consola	Se ejecuta el comando R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Se ejecuta el comando R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Se ejecuta el comando R3(config)#service password-encryption
Mensaje MOTD	Se ejecuta el comando R3(config)#banner motd #se prohibe el acceso no autorizado# R3(config)#
Interfaz S0/0/1	Se ejecutan los comandos

	R3(config)#int s0/2/1 R3(config-if)#ipv6 unicast-routing R3(config)#int s0/2/1 R3(config-if)#description conectado a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no sh
Interfaz loopback 4	Se ejecutan los comandos R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit %LINK-5-CHANGED: Interface Loopback4, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up R3(config)#
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit %LINK-5-CHANGED: Interface Loopback5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up R3(config)#
Interfaz loopback 6	Se ejecutan los comandos R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit %LINK-5-CHANGED: Interface Loopback6, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

	R3(config)#
Interfaz loopback 7	Se ejecutan los comandos interface loopback 7 ipv6 address 2001:DB8:ACAD:3::1/64 exit
Rutas predeterminadas	Se ejecutan los comandos R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)#ipv6 route ::/0 2001:db8:acad:2:::2

Fuente 10. Propia

Paso 5: Configurar S1

Se realiza la configuración básica teniendo en cuenta el nombre, protección por contraseña, encriptación del mensaje, la contraseña para acceso remoto se configura en line vty 0 15, con el comando "password" seguido de un espacio y la contraseña deseada, por último, el mensaje MOTD.

La configuración del S1 incluye las siguientes tareas:

Tabla 11Configuración S1 Paso 5

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecuta el comando Switch(config)#no ip domain-lookup Switch(config)#
Nombre del Switch	Se ejecuta el comando Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Se ejecuta el comando S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	Se ejecuta el comando S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	Se ejecuta el comando S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#
Cifrar las contraseñas de texto no cifrado	Se ejecuta el comando S1(config-line)#service password-encryption

Mensaje MOTD	Se ejecuta el comando S1(config)#banner motd #se prohibe el acceso no autorizado#

Fuente 11. Propia

Paso 6: Configurar S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12 Configuración S3 Paso 6

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Se ejecuta el comando Switch(config)#no ip domain-lookup
Nombre del Switch	Se ejecuta el comando Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	Se ejecuta el comando S3(config)#enable secret class
Contraseña de acceso a la consola	Se ejecuta el comando S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#
Contraseña de acceso Telnet	Se ejecuta el comando S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#
Cifrar las contraseñas de texto no cifrado	Se ejecuta el comando S3(config-line)#service password-encryption
Mensaje MOTD	Se ejecuta el comando S3(config)#banner motd #se prohibe el acceso no autorizado# S3(config)#

Fuente 12. Propia

Paso 7: Verificar la conectividad de la red

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

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

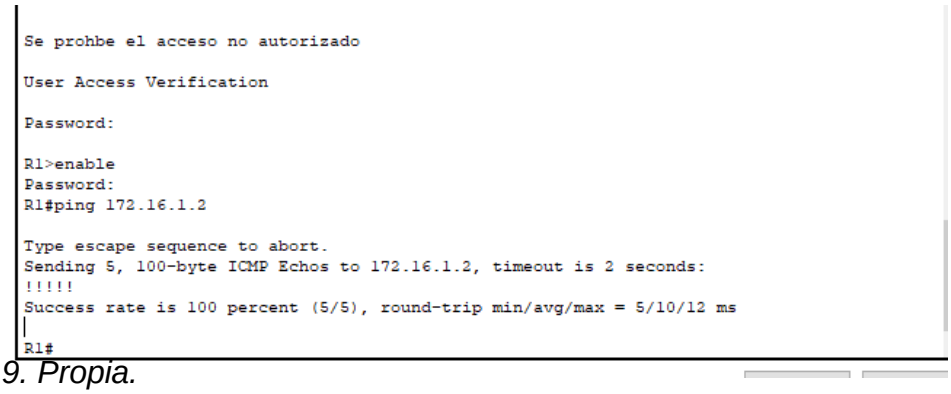
Tabla 13 Verificar Conectividad Paso 7

Desde	A	Dirección IP	Resultados de ping
R1	R2 S0/2/0	172.16.1.2	Exitoso
R2	R3, S0/2/1	172.16.2.1	Exitoso
PC de Internet	Gateway Predeterminado	209.165.200.238	Exitoso

Fuente 13. Propia

R1 Ping Exitoso

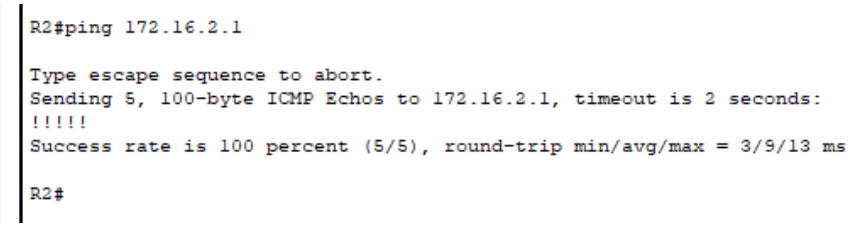
Figura 9. ping 172.16.1.2



Fuente: 9. Propia.

R2 ping Exitoso

Figura 10. R2-R3 Ping 172.16.2.1

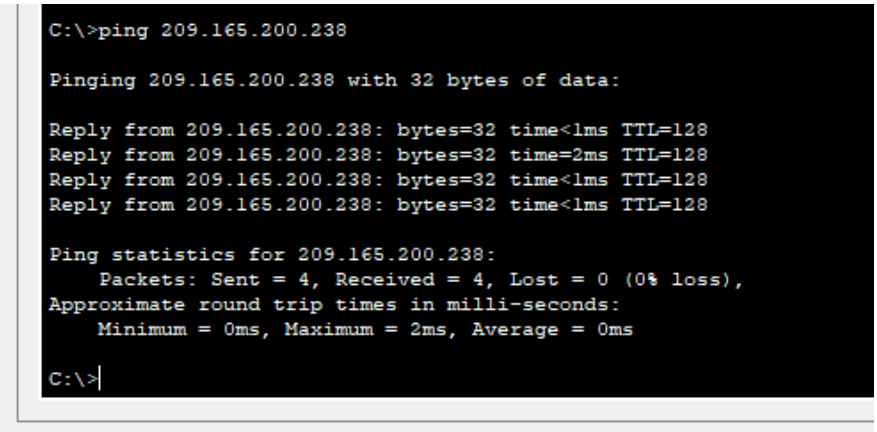


Fuente: 10 Propia.

Ping Gateway Predeterminado

Desde Pc de internet se hace ping al Gateway predeterminado, ip 209.165.200.238 arrojando como resultado la conectividad entre los dos dispositivos.

Figura 11. Ping 209.165.200.238



Fuente: 11 Propia.

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

Se crean las bases de datos para VLAN 21,23 y 99, se le asigna una dirección a la IP a la Vlan 99 designada como Administración, se asigna el Gateway predeterminado y se forzan los enlaces troncales para transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN. Luego se configuran los puertos como puertos de acceso y se asigna F0/6 a la VLAN 21.
Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración S1 Paso 1 Parte 3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Se ejecutan los comandos S1(config)#enable S1(config)#config t S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administración

	S1(config-vlan)#exit S1(config)#
Asignar la dirección IP de Administración	Se ejecutan los comandos S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no sh S1(config-if)#exit S1(config)#
Asignar el Gateway Predeterminado	Se ejecuta el comando S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Se ejecutan los comandos S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Forzar el enlace troncal en la interfaz F0/5	Se ejecutan los comandos S1(config)#int f0/5 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#enable S1#config t S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#exit S1(config)#exit
Asignar F0/6 a la VLAN 21	Se ejecutan los comandos S1#enable S1#config t S1(config)#int f0/6 S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	Se ejecutan los comandos S1#enable S1#config t S1(config)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#sh

Fuente 14. Propia

Paso 2: Configurar el S3

Se crean las bases de datos para VLAN 21,23 y 99, se le asigna una dirección a la IP a la vlan 99 denominada Administración, se asigna el gateway predeterminado y se forzan los enlaces troncales para transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN. Luego se configuran los puertos como puertos de acceso y se asigna F0/18 a la VLAN 23.

La configuración del S3 incluye las siguientes tareas:

Tabla 15 Configuración S3 Paso 2

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#enable S3#config t S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit S3(config)#exit
Asignar la dirección IP de Administración	Se ejecutan los comandos S3#enable S3#config t S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#exit S3(config)#exit
Asignar el Gateway Predeterminado	Se ejecuta el comando S3#enable S3#config t S3(config)#ip default-gateway 192.168.99.1 S3(config)#exit
Forzar el enlace troncal en la interfaz F0/3	Se ejecutan los comandos S3#enable S3#config t S3(config)#int f0/3 S3(config-if)#switchport mode trunk

	S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no sh S3(config-if)#exit S3(config)#exit
Configurar el resto de los puertos como puertos de acceso	Se ejecutan los comandos S3#enable S3#config t S3(config)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit S3(config)#exit
Asignar F0/18 a la VLAN 21	Se ejecutan los comandos S3#enable S3#config t S3(config)#int f0/18 S3(config-if)#switchport access vlan 23 S3(config-if)#exit S3(config)#exit
Apagar todos los puertos sin usar	Se ejecutan los comandos S3#enable S3#config t S3(config)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#sh S3(config-if-range)#exit

Fuente 15. Propia

Paso 3: Configurar R1

En el R1 se configura la subinterface en 802.1Q .21 en G0/1, la 802.1Q .23 en G0/1
y 802.1Q .99 en G0/1 y se activa la interfaz G0/1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16 Configuración R1 Paso3 Parte 3

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Se ejecutan los siguientes comandos R1(config)#int g0/0/1.21 R1(config-subif)#description Lan Contabilidad

	R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Se ejecutan los siguientes comandos R1#enable R1#config t R1(config)#int g0/0/1.23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Se ejecutan los siguientes comandos R1#enable R1#config t R1(config)#int g0/0/1.99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit R1(config)#exit
Activar la interfaz G0/1	Se ejecutan los siguientes comandos R1#enable R1#config t R1(config)#int g0/0/1 R1(config-if)#no sh

Fuente 16. Propia

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

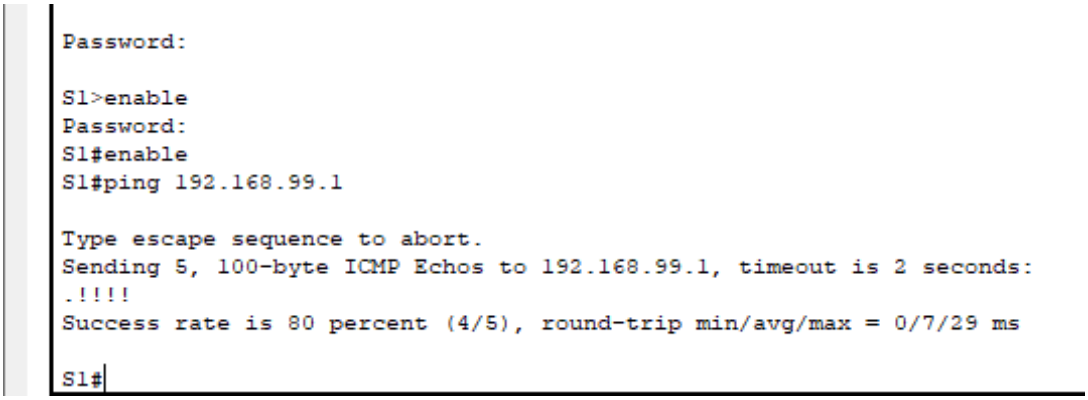
Tabla 17 Verificación de conectividad S1 y S3. Ping

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

S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

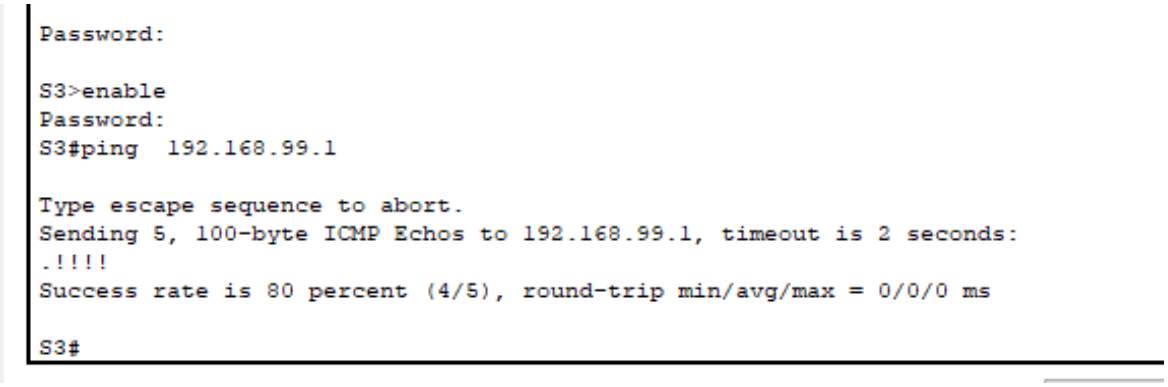
Fuente 17. Propia

Figura 12. Ping 192.168.99.1 S1 a R1 Vlan 99



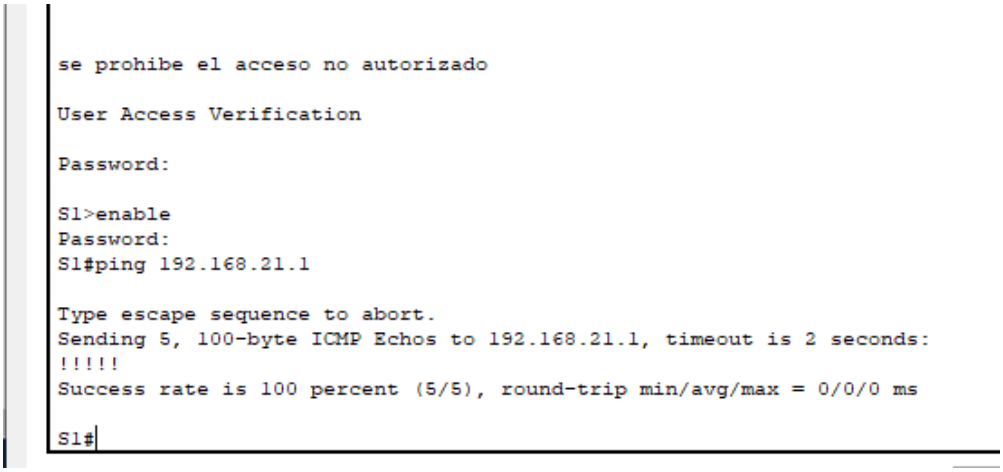
Fuente: 12 Propia.

Figura 13. Ping 192.168.99.1 S3 a R1 Vlan 99



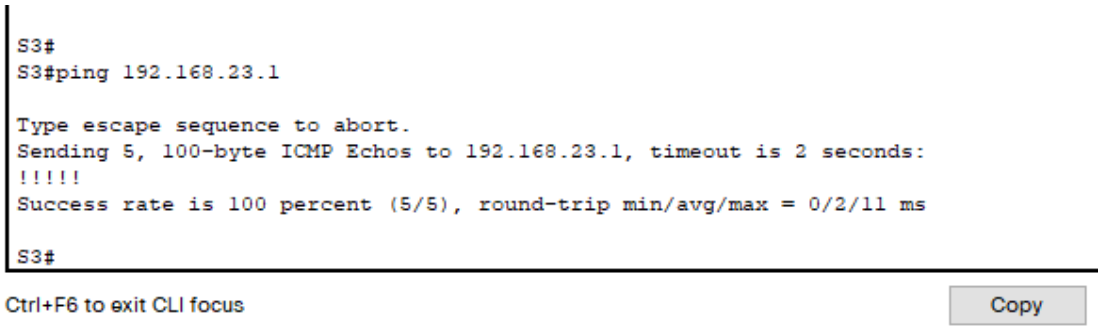
Fuente: 13 Propia.

Figura 14. Ping 192.168.21.1 S1 a R1 Vlan 21



Fuente: 14 Propia.

Figura 15. Ping 192.168.23.1 S3 a R1 Vlan 23



Fuente: 15 Propia.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Se configura la OSPF en al área 0 lo que hace que el router dentro de un área mantiene la información completa de la topología del área. Se anuncian las redes conectadas directamente y las interfaces LAN se establecen como pasivas

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R1>enable Password: R1#enable R1#config t R1(config)#router ospf 47 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	Se ejecutan los comandos R1#enable R1#config t R1(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R1(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R1(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R1(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R1(config)#access-list 1 permit 192.168.6.1 0.0.0.255
Establecer todas las interfaces LAN como pasivas	Se ejecutan los comandos R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99 R1(config-router)#exit R1(config)#ipv6 unicast-routing R1(config)#ipv6 router ospf 47 R1(config-rtr)#router-id 1.1.1.1 R1(config-rtr)#exit R1(config)#interface s0/2/0 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 ospf 47 area 0
Desactive la sumarización automática	En ospf no se puede hacer de acuerdo a la web conferencia de fecha 15 de Noviembre de 2021 El comando es R1(config-router)#No auto-summary

Fuente 18. Propia

Paso 2: Configurar OSPF en el R2

OSPF es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF)

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configuración OSPF en R2 Paso 2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R2#enable R2#config t R2(config)#router ospf 47 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#exit
Establecer todas las interfaces LAN (loopback)como pasivas	Se ejecutan los comandos R2(config-router)#passive-interface loopback 0 R2#enable R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ipv6 unicast-routing R2(config)#int g0/0/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#exit R2(config)#int s0/2/0 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#exit R2(config)#int s0/2/1 R2(config-if)#ipv6 address fe80::2 link-local R2(config-if)#exit R2(config)#ipv6 router ospf 47 R2(config-rtr)#router-id 2.2.2.2

	R2(config-rtr)#auto-cost reference-bandwidth 1000 % OSPF: Reference bandwidth is changed. Please ensure reference bandwidth is consistent across all routers. R2(config-rtr)#exit R2(config)#int g0/0/0 R2(config-if)#ipv6 ospf 47 area 0 R2(config-if)#exit R2(config)#int s0/2/0 R2(config-if)#ipv6 ospf 47 area 0 R2(config-if)#exit R2(config)#int s0/2/1 R2(config-if)#ipv6 ospf 47 area 0 R2(config-if)#exit R2(config)# 03:43:51: %OSPFv3-5-ADJCHG: Process 47, Nbr 1.1.1.1 on Serial0/2/0 from LOADING to FULL, Loading Done R2(config)#
Desactive la sumarización automática	NO se puede hacer en este sistema de enrutamiento, solo se hace en rip y en EIGRP la sumarización automática

Fuente 19. Propia

Paso 3: Configurar OSPFv3 en el R3

En el paso 3 Configurar ospfv3 en R2 no se hace anunciar redes ipv4 sino ipv6 de acuerdo a las indicaciones dadas en la webconferencia ya que existe error en la guía, error esto debe ser para las redes bajo IPV6.

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración R3 Paso 3

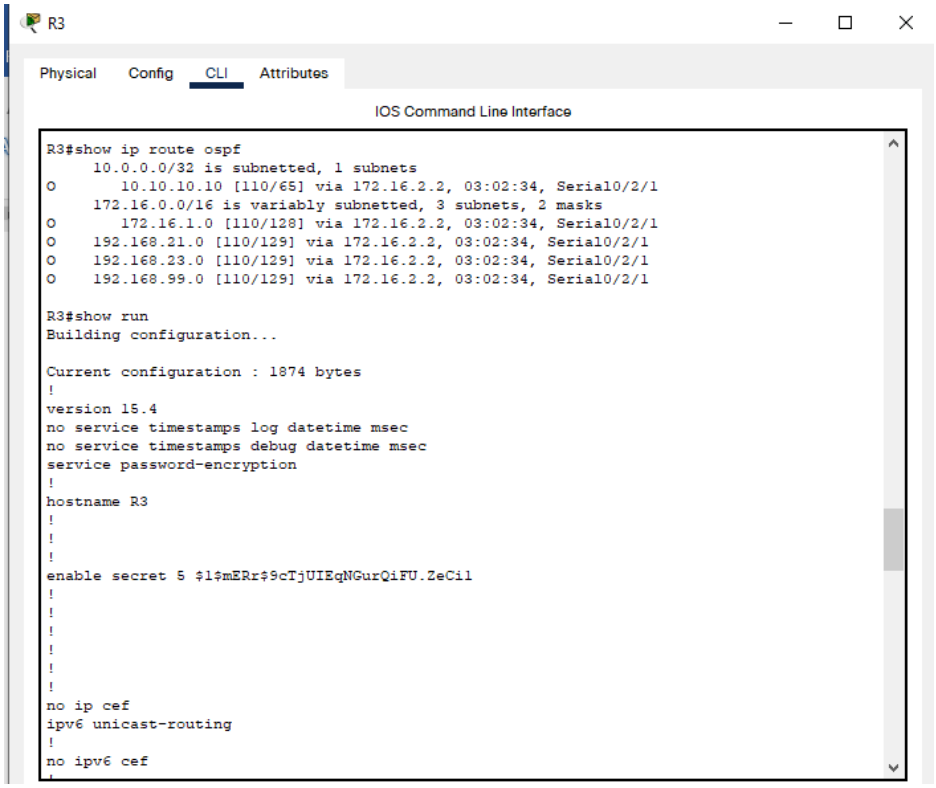
Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Se ejecutan los comandos R3#enable R3#config t R3(config)#router ospf 47 R3(config-router)#router-id 3.3.3.3

Anunciar las redes IPV4 conectadas directamente	Se ejecutan los comandos R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#exit R3(config)#exit
Establecer todas las interfaces LAN IPV4 (loopback)como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3#enable R3#config t Enter configuration commands, one per line. End with CNTL/Z. R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 47 R3(config-rtr)#router-id 3.3.3.3 R3(config-rtr)#int s0/2/1 R3(config-if)#ipv6 ospf 47 area 0 R3(config-if)# 03:57:14: %OSPFv3-5-ADJCHG: Process 47, Nbr 2.2.2.2 on Serial0/2/1 from LOADING to FULL, Loading Done R3(config-if)#ipv6 address fe80::3 link-local R3(config-if)# 03:57:40: %OSPFv3-5-ADJCHG: Process 47, Nbr 2.2.2.2 on Serial0/2/1 from LOADING to FULL, Loading Done R3(config-if)#int loopback 7 R3(config-if)#ipv6 address fe80::3 link-local R3(config-if)#ipv6 ospf 47 area 0 R3(config-if)#exit R3(config)#exit R3#

	%SYS-5-CONFIG_I: Configured from console by console
Desactive la sumarización automática	NO se puede hacer en este sistema de enrutamiento, solo se hace en rip y en EIGRP la sumarización automática

Fuente 20. Propia

Figura 16. Configuración R3



Fuente: 16 Propia

Paso 4: Verificar la información de OSPF

En el R2 se ejecuta el comando show ip protocols donde muestra la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router

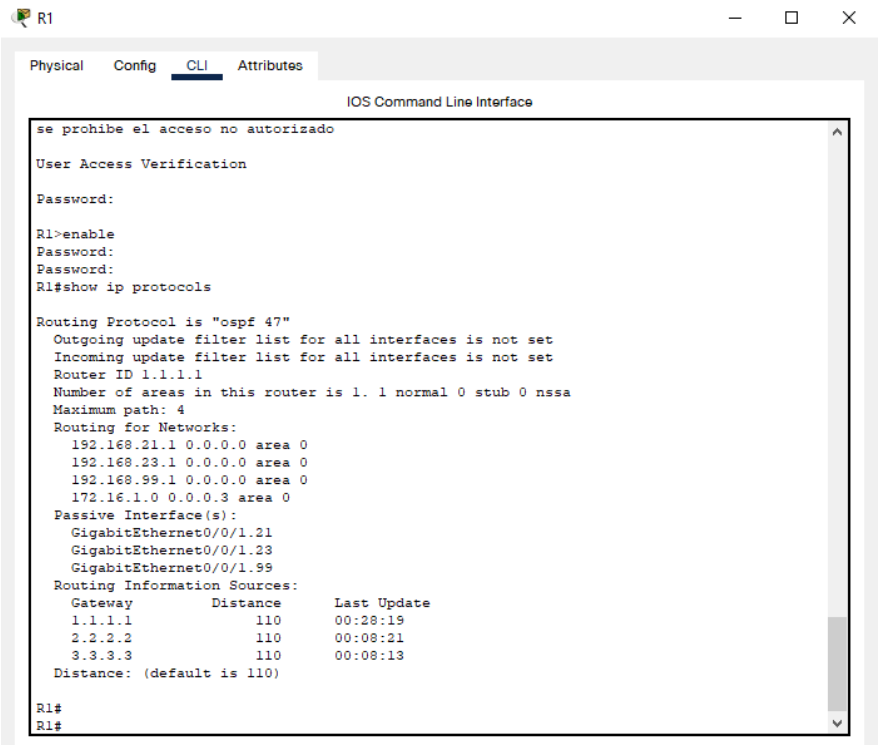
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Verificación Información OSPF Paso 4

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show running-config

Fuente 21. Propia

Figura 17. Verificación OSPF.



Fuente: 17 Propia

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 Configurar R1 -servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Se ejecuta el comando R1#enable R1#config t 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	Se ejecuta el comando R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Se ejecutan los comandos R1#enable R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 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 R1(dhcp-config)#end
Crear un pool de DHCP para la VLAN 23	Se ejecutan los comandos R1#enable R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 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 R1(dhcp-config)#end R1#

Fuente 22. Propia

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Paso 2: Configuración de NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Se ejecutan los comandos R2>enable Password: R2#config t R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	eso es un error de comando ip http server comando no sirve ip http server R2(config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)#
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Comando no soportado en Packet Tracer R2#config t Enter configuration commands, one per line. End with CNTL/Z. ip http authentication local ^ % Invalid input detected at '^' marker. R2(config)#
Defina el pool de direcciones IP públicas utilizables. Definir la traducción de NAT dinámica	Se ejecuta el comando 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	Se ejecutan los comandos R2#enable R2#config t

	R2(config)#interface loopback 0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#int s0/2/0 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#int s0/2/1 R2(config-if)#ip nat inside R2(config-if)#exit R2(config)#int g0/0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#exit R2#
Defina el pool de direcciones IP públicas utilizables. Definir la traducción de NAT dinámica	Se ejecutan los comandos R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255 R2(config-if)#exit
Defina el pool de direcciones IP públicas utilizables.	Se ejecuta el comando R2#enable R2#config t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#exit
Definir la traducción de NAT dinámica	Se ejecuta el comando R2#enable R2#config t R2(config)#ip nat inside source list 1 pool INTERNET

Fuente 23. Propia

Paso 3: Verificar el protocolo DHCP y la NAT estática

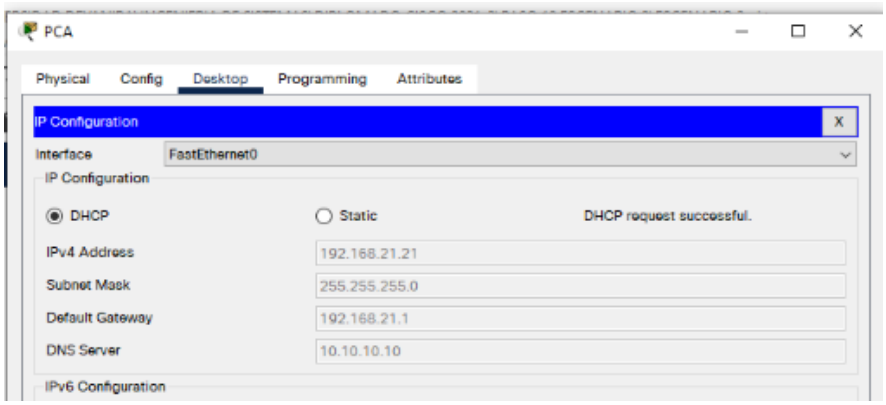
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 24. Paso 3 Verificar Protocolo DHCP y NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	192.168.21.21 255.255.255. 0
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC	ping 192.168.23.21
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	Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: A small page Copyrights Image page Image

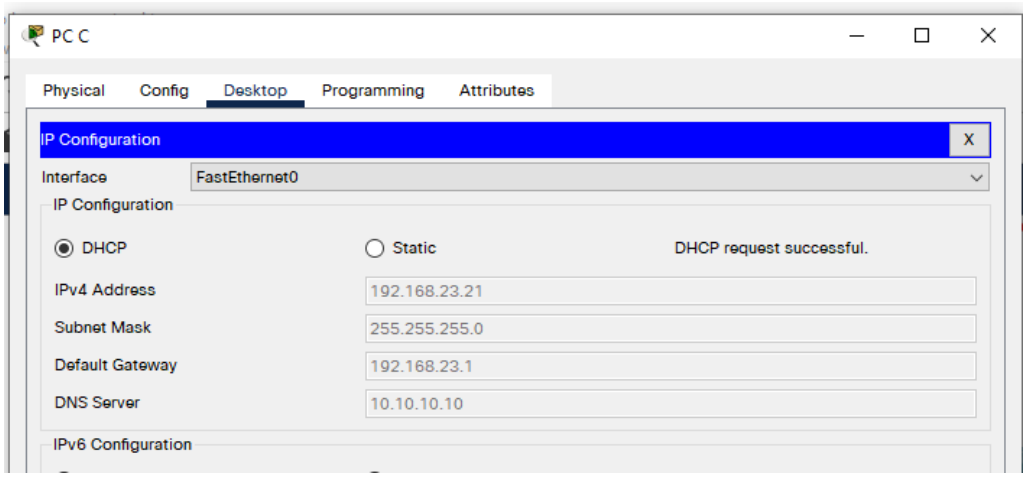
Fuente 24. Propia

Figura 18. Verificación Protocolo DHCP PC-A



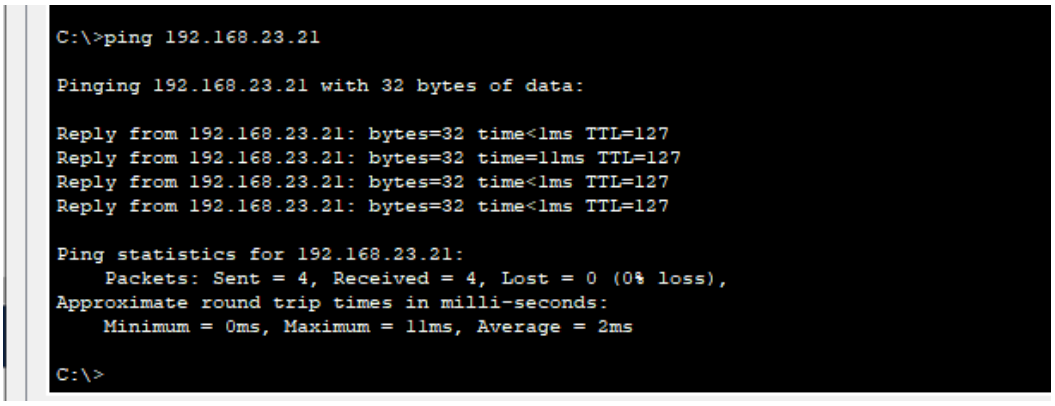
Fuente: 18. Propia

Figura 19. Verificación Protocolo DHCP PC-C



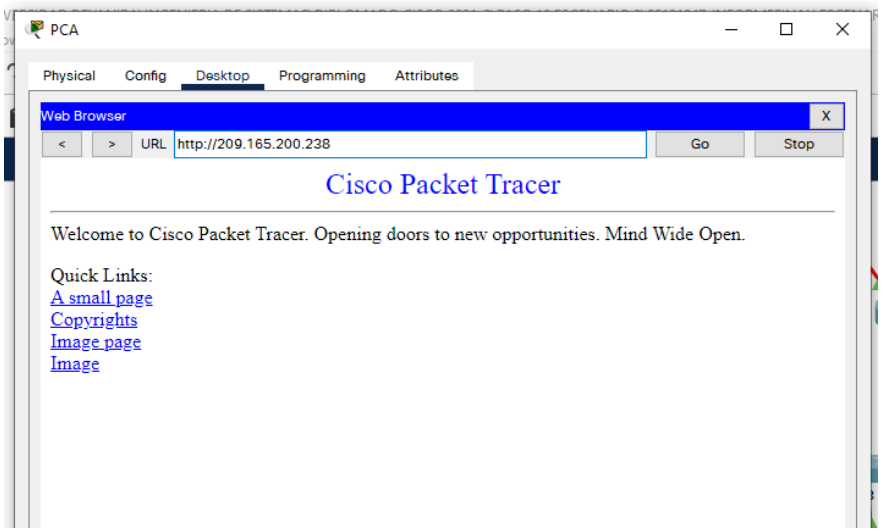
Fuente: 19. Propia

Figura 20. PC-A ping PC-C 192.168.23.21



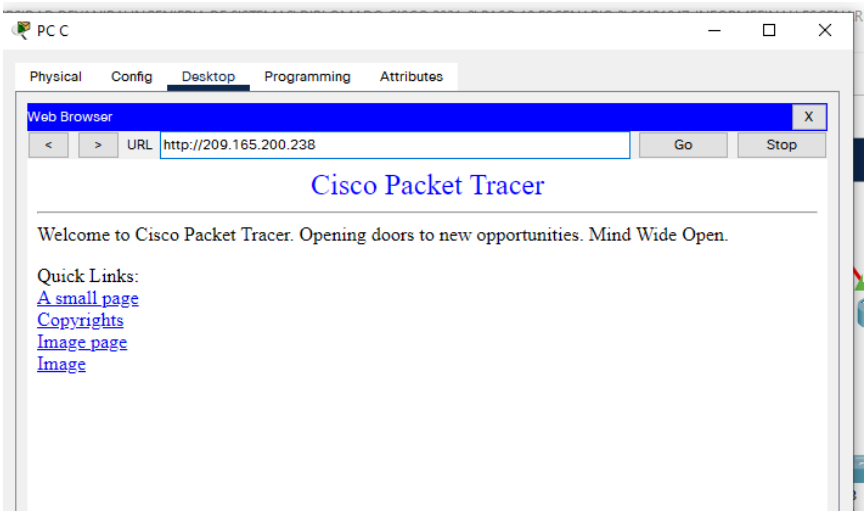
Fuente: 20. Propia

Figura 21. PC-A 209.165.200.238



Fuente: 21. Propia

Figura 22. PC-C 209.165.200.238



Fuente: 22. Propia

Parte 6: Configurar NTP

El NTP es un protocolo para sincronizar varios relojes de red usando un conjunto de clientes y servidores repartidos. El NTP proporciona los mecanismos de protocolo básicos necesarios para sincronizar los relojes de los diferentes sistemas

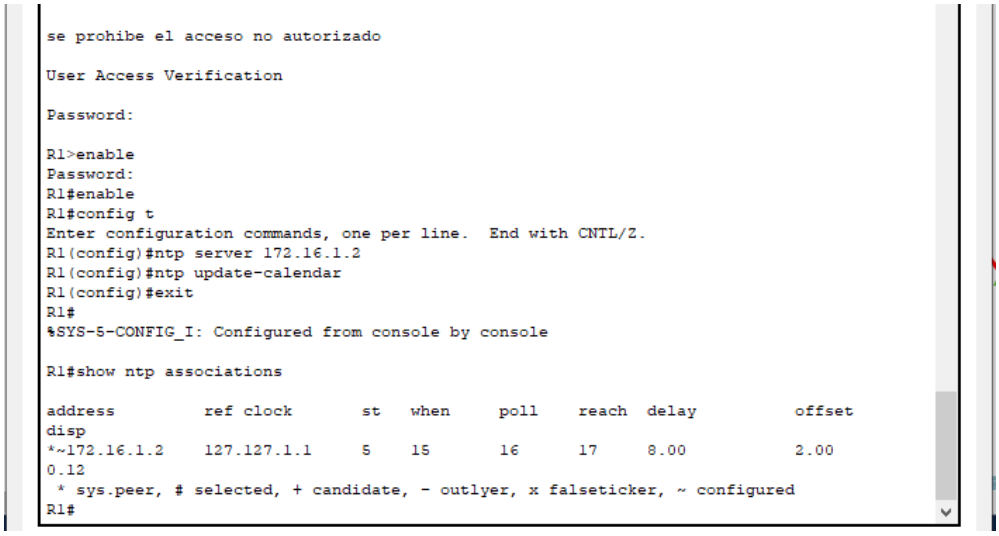
con una precisión del orden de nanosegundos. Además, contiene indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local. Es así que realiza la configuración de la fecha en el R2, se configura como maestro y luego en el R1 como cliente NTP, las actualizaciones de calendario periódicas con NTP.

Tabla 25. Configuración NTP Parte 6

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2	Se ejecuta el comando R2#clock set 09:00 05 march 2016
Configure R2 como un maestro NTP.	Se ejecutan los comandos R2#enable R2#config t R2(config)#ntp master 5 R2(config)#exit
Configurar R1 como un cliente NTP.	Se ejecutan los comandos R1>enable R1#config t R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Se ejecuta el comando R1(config)#ntp update-calendar R1(config)#exit
Verifique la configuración de NTP en R1	Se ejecuta el comando R1#show ntp associations

Fuente 25. Propia

Figura 23. Configuración NTP



Fuente: 23. Propia

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

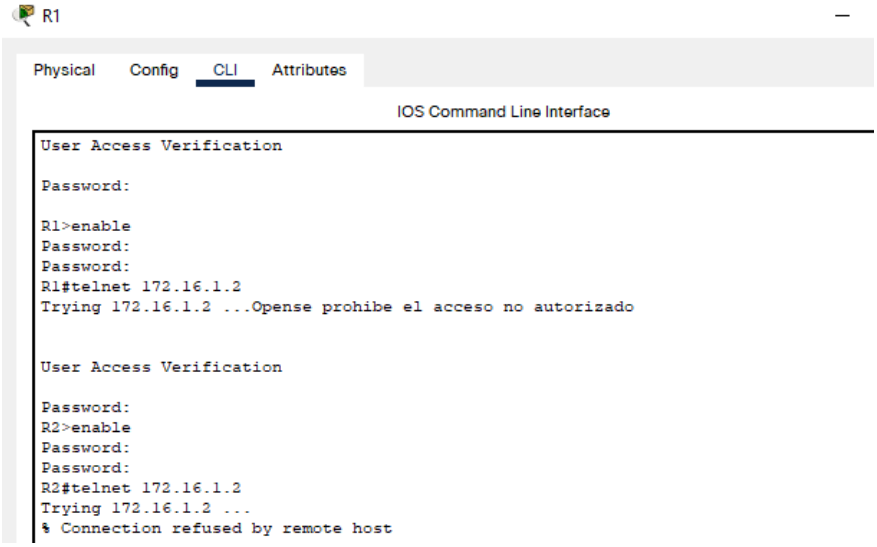
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Restricción de acceso lineas VTY en 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	Se ejecutan los comandos R2#enable R2#config t R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	Se ejecutan los comandos R2#enable R2#config t R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#
Permitir acceso por Telnet a las líneas de VTY	Se ejecutan los comandos R2(config-line)#transport input telnet R2(config-line)#
Verificar que la ACL funcione como se espera	Se ejecutan los comandos R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Opense prohibe el acceso no autorizado User Access Verification Password: R2#telnet 172.16.1.2 Trying 172.16.1.2 ... % Connection refused by remote host R2#

Fuente 26. Propia

Figura 24. Verificación Telnet R1 172.16.1.2



Fuente 24. Propia

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

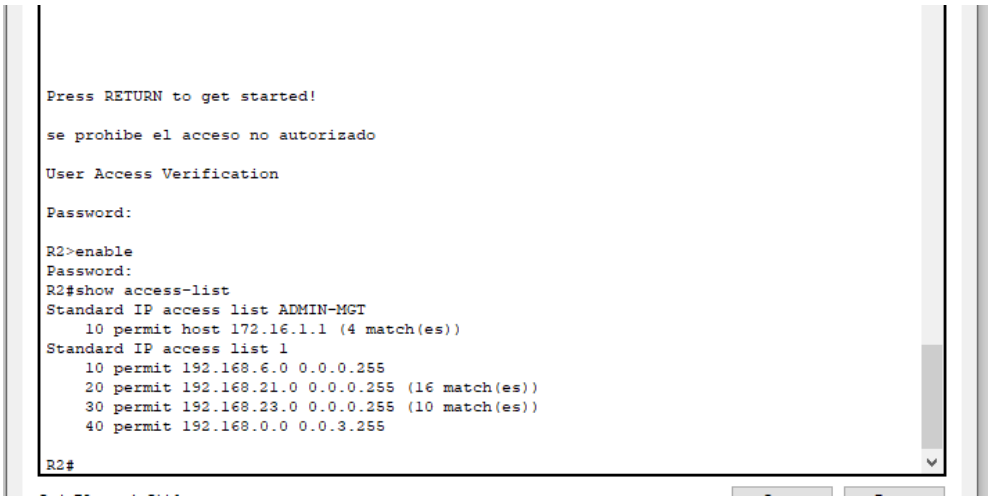
Tabla 27. Comando CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Se ejecutan los comandos R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (16 match(es)) 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 40 permit 192.168.0.0 0.0.7.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 R2#
Restablecer los contadores de una lista de acceso	Se aplica el comando clear ip access-list counters show access-list se deja un espacio al iniciar y lo toma

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Se ejecuta el comando R2# show ip interface s0/2/0
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Se aplican los comandos R2#clear ip nat translations

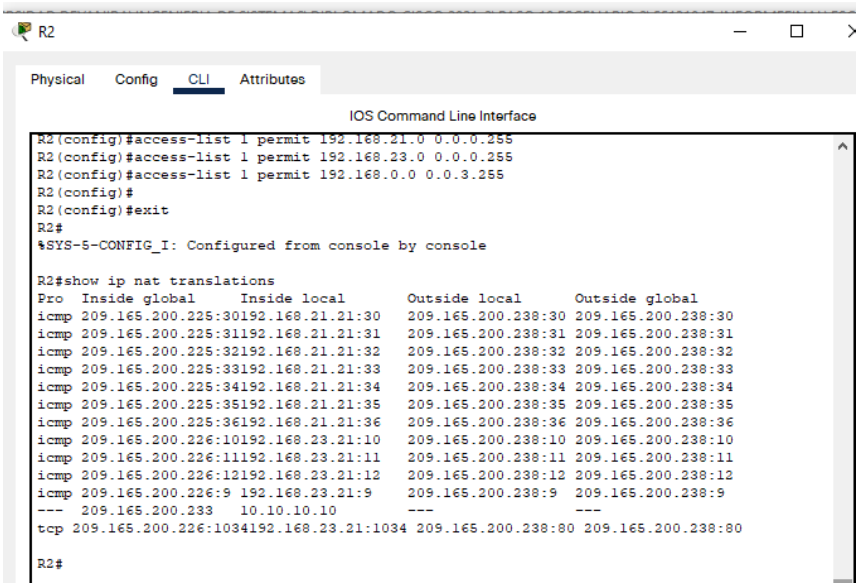
Fuente 27. Propia

Figura 25. Comando Show Access-list



Fuente: 25. Propia

Figura 26. Comando Show ip nat Translations



Fuente: 26. Propia

CONCLUSIONES

Con el desarrollo del presente informe y la aplicación de los dos escenarios se ha logrado profundizar los diferentes temas de configuración de Router, Switch, además de los pcs, demostrando la conectividad de la red, por medio de direccionamiento IPV4

Así mismo, se lograron identificar muchas falencias que se tenían en cuanto a la aplicación de los comandos en cada una de las configuraciones de red, generando la necesidad de verificación e investigación para aplicarlos debidamente.

Se afianzaron varios temas de direccionamiento los cuales se tenían nociones muy limitadas por su poca aplicación en situaciones de la vida cotidiana y de manejo de configuraciones de redes, se obtuvo mayor familiaridad con la aplicación de cada comando, además me exigió desarrollar la habilidad de búsqueda y profundizar un poco más en el tema, encontrando información importante a tener en cuenta en el desarrollo de nuevos ejercicios y configuraciones de redes en tiempo real y mediante el uso del simulador Packet Tracer.

Se concluye con el desarrollo de este proyecto realizado la obtención de los conocimientos necesarios para la configuración y simulación de una red ISP (Proveedor de servicios de internet) con todos los lineamientos necesarios para dar servicio de internet a diferentes empresas que requieran del servicio.

Como último punto, y no menos importante se contó con el apoyo del tutor asignado y la directora de curso, quienes con su colaboración y paciencia han dedicado y aportado sus conocimientos para obtener las bases teóricas para desarrollar los escenarios propuestos de la mejor manera.

BIBLIOGRAFIA

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84.

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

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

CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

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

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

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

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, *12*(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)* (pp. 1-6). IEEE.

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3