IMPLEMENTACION DE 2 REDES CORPORATIVAS CON TECNOLOGÍA CISCO

EINAR ALEJANDRO ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
NOVIEMBRE DEL 2020.

IMPLEMENTACION DE 2 REDES CORPORATIVAS CON TECNOLOGÍA CISCO.

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR POR EL TITULO DE INGENIERO DE SISTEMAS

EINAR ALEJANDRO ROJAS

TUTOR
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
NOVIEMBRE DEL 2020.

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____
FIRMA

_____
FIRMA

_____
FIRMA

A lo largo de éste camino estudiantil he aprendido cosas importantes que facilitan el desarrollo de mis actividades laborales, ésta meta no habría Sido posible lograrla sin el apoyo de mi familia ya que por ellos es que he logrado cumplir cada meta propuesta. Por otro lado agradezco a los tutores que han hecho posible el proceso de aprendizaje continuo dentro de ésta institución.

EINAR ALEJANDRO ROJAS.

AGRADECIMIENTOS

Me encuentro en un punto muy importante de mi vida, estoy a un pequeño paso de cumplir esta nueva meta lo cual solo ha sido posible gracias a la intervención de Personas, Profesores e Instituciones que nos han aportado una serie de elementos que han favorecido nuestra formación, agradezco enormemente todo ese tiempo que nos han brindado y por ese apoyo que nos han suministrado cuando más lo hemos necesitado.

Le agradezco infinitamente a Dios por ser uno de los artífices dentro de cada uno de los pasos que he dado, por brindarme esa paciencia que necesito, por haberme brindo la sabiduría necesaria para terminar esta actividad de la mejor manera. A cada uno de mis familiares, pues definitivamente han sido ese puntal que he necesitado muchas veces al darme la mano, levantarme y seguir luchando.

A mis compañeros les agradezco por haber compartido tanto tiempo conmigo, por haber superado tantas adversidades, momentos muy complicados que solo con el apoyo incondicional de cada uno de ellos fue posible superar, les agradezco y comparto mi alegría pues muchos de ellos también están con migo finalizando sus actividades académicas.

A todos mis tutores que aportaron a mi formación. Para quienes me enseñaron más que el saber científico, sino que me enseñaron a ser lo que no se aprende en salón de clase y a compartir el conocimiento con los demás.

Tabla de Contenido

Glosario 10
Resumen 16
Introducción 17
Justificación 18
Objetivos 19
Objetivo general 19
Objetivos Específico 19
CASO DE ESTUDIO: ESCENARIO 1 20
Escenario 1 20
Topología 20
Instrucciones 23
Paso 1: Configurar R1 23
Tabla 3: CONFIGURACIÓN ROUTER 1 26
Paso 2: Configure S1 y S2. 28
Paso 3: Configure S1 y S2. – minuto 25-58 30
Paso 4: Configurar S1 32
Paso 5: Configure el S2. 37
Parte 2: Configurar soporte de host 40
Paso 1: Configure R1 40
Paso 2: Configurar los servidores 43
Parte 3: Probar y verificar la conectividad de extremo a extremo 46
4. ESCENARIO 2. 52
Escenario 2 52
Parte 1: 53
Parte 3: 66
Parte 4: 73
Parte 5: 78
Parte 6: 83
Parte 7: 84

PING Y TRACEROUTE. 87
SIMULADOR....87
CONCLUSIONES 88
BIBLIOGRAFIA Y WEBGRAFIA 89
BIBLIOGRAFIA 89

Contenido De Figuras

Figura 1: TOPOLOGIA ESCENARIO 1....21
Figura 2: TOPOLOGIA ESCENARIO 1....21
Figura 3: Configuración Del R1. 27
Figura 4: Configuración Del S1. 36
Figura 5....44
Figura 6....45
Figura 7 - Verificación De DHCP En Las PC. 45
Figura 8....48
Figura 9 - Pruen De Conectividad Desde PC-A 49
Figura 10 - Pruen De Conectividad Desde PC-A 49
Figura 11 - Prueba Puerta De Enlace IPV6 50
Figura 12....51
Figura 13 - Prueba De Conectividad IPV6 52
Figura 14 - Prueba De Conectividad IPV6 52
Figura 15 - TOPOLOGIA ESCENARIO 2. 53
Figura 16 - Prueba De Conectividad S1 Y S2. 73
Figura 17 - Show Protocols R1. 76
Figura 18 - Show Ip Route Ospf En R1....77
Figura 19 - Show Running-Config En R1....77
Figura 20 - Verificación DHCP En PC-A. 82
Figura 21 - Verificación DHCP En PC-C. 82

Figura 22 - PING Desde PC-A. 83
Figura 23 - Verificación De ACL EN R2 86
Figura 24 - Verificación NAT En R2 86

Contenido De Tablas

Tabla De VLAN 21
Tabla 1: TABLA DE VLAN ESCENARIO 1. 22
Tabla De Asignación De Direcciones 22
Tabla 2: TABLA DE ASIGNACION DE DIRECCIONES 22
Tabla 3: CONFIGURACIÓN ROUTER 1 26
Tabla 4: CONFIGURACIÓN INTERFACES ROUTER 1 27
Tabla 5: CONFIGURACIÓN SWITCH 1 29
Tabla 6: CONFIGURACIÓN SWITCH 2 32
Tabla 7: CONFIGURACIÓN SWITCH 1 - *(VLAN, Trunking, Etherchannel)* 36
Tabla 8: CONFIGURACIÓN SWITCH 2 - (VLAN, Trunking, Etherchannel) 39
Tabla 9: CONFIGURACIÓN ROUTER 1 - Loopback 0 - DHCP 42
Tabla 10: CONFIGURACIÓN DHCP PC-A – PC-C 46
Tabla 11: Pruebas De Conectividad. 48
Tabla 12: Reinicializar Dispositivos. 54
Tabla 13- CONFIGURACIÓN Computadora De Internet 55
TABLA 14 - Configuración Básica R1 57
TABLA 15 - Configuración Básica R2 61
TABLA 16 - Configuración Básica R3 63
TABLA 17 - Configuración Básica S1 64
TABLA 18 - Configuración Básica S3 65
TABLA 19 - Prueba Conectividad, Dispositivos Directos. 66
TABLA 20 - S3 – Vlans, Interfaces, Enlaces Trunk 70
TABLA 21 - R1 – Configuración Vlans, Interfaces. 72

TABLA 22 Prueba De Conectividad.....72
TABLA 23 Configurar OSPF R1.....74
TABLA 24 Configurar OSPF R2.....74
TABLA 25 Configurar OSPF R3.....75
TABLA 26 - Configurar El R1 Como Servidor De DHCP 79
TABLA 27 - Configurar La NAT Estática Y Dinámica EN R2 80
TABLA 28 - Verificación De DHCP Y NAT.....82
TABLA 29 - Configuración De NTP.....84
TABLA 30 - Configuración De Restrocciones En R2 84
TABLA 31 - Comandos CLI.....85

Glosario

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

Acceso Universal. Es el derecho que tienen todos los usuarios de TPBC a comunicarse con cualquier otro usuario de la red de telecomunicaciones del Estado y de cualquier otra red de telecomunicaciones en el exterior.

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

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

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

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

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

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

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

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

CSMA Carrier Sense Multiple Access. Acceso Múltiple por Detección de Portadora. Protocolo de Red para compartir un canal. Antes de transmitir la estación emisora comprueba si el canal esta libre.

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

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

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

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

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

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

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

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

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

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

ISO International Standard Organization. Organización Internacional de Estándares.

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

Cable de fibra óptica: un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

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

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

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

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

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

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

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

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

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

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

Router: dispositivo intermediario en las redes que se asegura de que la información no va a donde no es necesario; la labor principal de un Router es

disipar y coordinar la información perteneciente a las direcciones lógicas de Red en un sistema.

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

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

Resumen

En el desarrollo de este Diplomado de profundización he adquirido muchos conocimientos los cuales fueron aplicados en el desarrollo de estos 2 escenarios. Trabajo en el cual nos ha permitido que conozcamos mucho más cada uno de los dispositivos que hacen parte de las redes de datos, los medios que permiten conectarlos tanto, físicos, como no físicos. Aplicare todo el conocimiento adquirido en lo que tiene que ver con el direccionamiento IP aplicando VLSM tanto para el direccionamiento IPV4 como también IPV6.

En este curso hemos adquirido mucha experiencia a la hora de emplear la herramienta de PACKET TRACER la cual ha sido la posibilidad perfecta para las personas que no disponemos de esos dispositivos físicos en los cuales podamos aplicar nuestro conocimiento. PACKET TRACER ha sido ese medio para adentrarnos en la IOS de los diferentes dispositivos de la red y así poder configurarlos de acuerdo a las exigencias de cada uno de los escenarios.

Se practicará con una serie de conceptos de redes como lo son el direccionamiento y enrutamiento. Con relación al direccionamiento practicaremos con la utilización de VLSM, además realizaremos la respectiva documentación con el fin de tener un soporte escrito y bien documentado de los pasos realizados. Ya en la parte del enrutamiento abordaremos el estudio de una se comandos y diferentes tipos de protocolos que nos ofrecen diferentes posibilidades dependiendo de las circunstancias en la cual lo queremos emplear.

Introducción

La industria de la tecnología en muy poco tiempo ha logrado ganar un espacio muy grande dentro de las vidas cotidianas, tanto a nivel personal como a nivel de las organizaciones, ya de nada sirve ese viejo modelo de tener las cosas guardadas solo para mí, el conocimiento y la información siempre debe estar disponible a la mano, todo debe estar conectado y funcionando las 24 horas del día los 7 días de la semana. Actualmente todos debe estar conectado, la gran mayoría de veces no directamente sino gracias a la redes de datos las cuales emplean un sinnúmero de medios tanto físicos como otros que no lo son, son muchas las posibilidades, entre ellas hilo de cobre, el uso de láser, microondas, fibra óptica y satélites de comunicaciones entre muchas otras más.

En el presente trabajo lo que vamos a desarrollas son 2 ESCENARIOS los cuales se nos entregan con una serie de exigencias gracias a los cuales vamos a poder aplicar todas esas habilidades que hemos adquirido a lo largo de nuestra carrera como también en el DIPLOMADO. Toda la parte práctica, configuración y montaje de cada uno de estos escenarios será realizada dentro del simulador de PACKET TRACER el cual nos ha permitido conocer la IOS de los diferentes dispositivos que hacen parte de la red de datos, configurar sus diferentes opciones y además generar en cada uno de nosotros esas destrezas que son de suma importancia para nuestra vida profesional.

Ahora el presente trabajo tiene unos objetivos bien delimitados y claros, el primero que podamos practicar todo lo que hemos adquirido y el segundo que lo podamos hacer en casos que acerquen bastante a la realidad. Un primer caso de estudio que nos brinda una inducción al direccionamiento IP y tablas de direccionamiento, y un segundo caso en el cual practicamos todo lo anterior junto con los protocolos de enrutamiento que nos lo permitan

Espero el trabajo sea de su agrado.

Justificación

En la actualidad es de vital importancia para todo ingeniero de sistemas manejar perfectamente los conceptos básicos y la forma de configurar todos los equipos utilizados en las redes computacionales. Esto nos forma de una manera mucha más integra para un mercado que está creciendo, debemos estar siempre a la vanguardia.

Es muy importante que como profesionales practiquemos constantemente. Todo el conocimiento se afianza en nosotros de esta manera. Es por esto que de mi parte con el desarrollo de estas 2 practicas busco que todas las habilidades que a lo largo del Diplomado adquirí sean empleadas en la solución de aspectos reales que muy seguramente vamos a afrontar dentro de nuestra vida profesional.

Nuestros conocimientos serán afianzados y nuestras dudas serán aclaradas.

Objetivos

Objetivo general

Analizar, resolver e implementar los ESCENARIO 1 Y 2 mediante la utilización de la herramienta de simulación de redes PACKET TRACER proporcionando una excelente conectividad entre todos los dispositivos de las redes.

Objetivos Específico

- Demostrar que el proceso de estudio autónomo, es un beneficio para aquellas personas que no cuentan con tiempo para ampliar el saber.
- Comprender la importancia de trabajar en grupo como una herramienta poderosa a la hora de lograr los objetivos planteados.
- Profundizar mucho más en el manejo de la herramienta de PACKET TRACER.
- Configurar los dispositivos finales e intermediarios en las redes.
- Conocer los diferentes protocolos de enrutamiento y envío de paquetes entre redes, teniendo en cuenta el uso y administración adecuado del Sistema Operativo de Internet working (IOS).

CASO DE ESTUDIO: ESCENARIO 1

3.1 Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

Topología

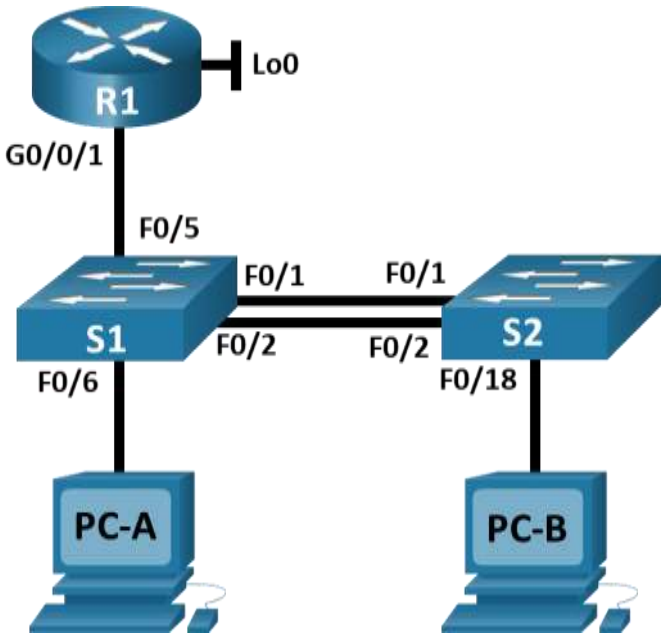

Figura 1: TOPOLOGIA ESCENARIO 1

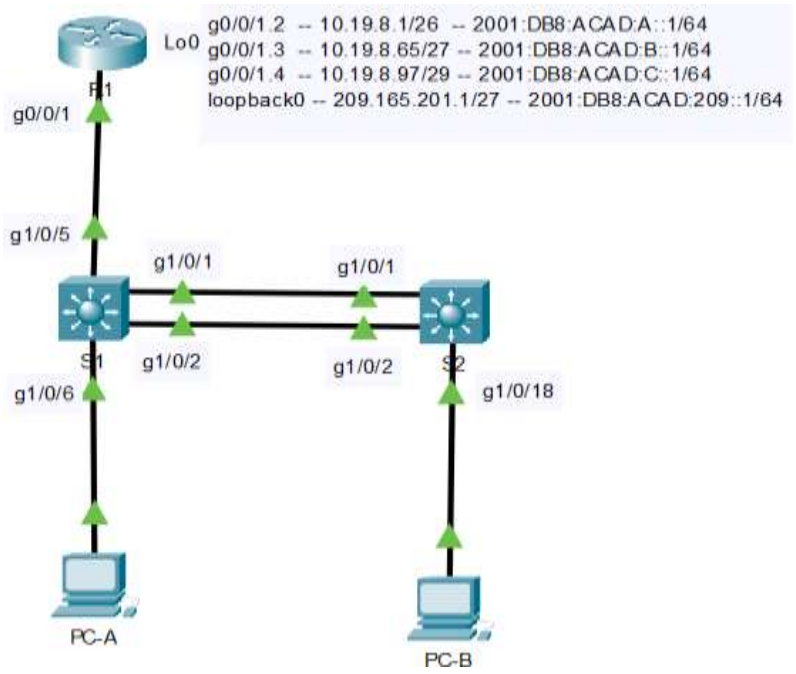

Figura 2: TOPOLOGIA ESCENARIO 1

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 de VLAN

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

Tabla 1: TABLA DE VLAN ESCENARIO 1.

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
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	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
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Tabla 2: TABLA DE ASIGNACION DE DIRECCIONES.

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

Instrucciones

Parte: 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.

  S1

  Erase-startup-config

  Delete vlan.dat

  Reload

  S2

  Erase-startup-config

  Delete vlan.dat

  Reload

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

  Show sdm prefer

  Vemos que soporta IPV6

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

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	Hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass Enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass Line console 0 Password ciscoconpass login
Establecer la longitud mínima para las contraseñas	10 caracteres Security passwords min-leng 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vt 0 15 login local
Configurar VTY solo aceptando SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configure un MOTD Banner	Banner motd %_____%
Habilitar el routing IPv6	Ipv6 unicast-routing

	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz. Int g0/0/1.2 Encapsulation dot1q 2 Description BIKES Ip addres 10.19.8.1 255.255.255.192 Ipv6 addres 2001:db8:acad:a:1/64 Ipv6 addres fe80::1 link local Int g0/0/1 No shutdown Int g0/0/1.3 Encapsulation dot1q 3 Description TRIKES Ip addres 10.19.8.65 255.255.255.224 Ipv6 addres 2001:db8:acad:b:1/64 Ipv6 addres fe80::1 link local Int g0/0/1.4 Encapsulation dot1q 4 Description MANAGEMENT Ip addres 10.19.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local Int g0/0/1.6 Encapsulation dot1q 6 NARIVE Description NATIVE Ip addres 10.19.8.97 255.255.255.224 Ipv6 addres 2001:db8:acad:c:1/64 Ipv6 addres fe80::1 link local
Configurar interfaz G0/0/1 y subinterfaces	Int g0/0/1

Tarea	Especificación
	No shutdown
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1** Interface loopback 0 Ip address 209.165.201.1 255.255.255.224 Ipv6 address 2001:db8:acad:209::1/64 Ipv6 address fe80::1 link-local Description INTERNET
Generar una clave de cifrado RSA	Módulo de 1024 bits Crypto key generate rsa modulus 1024

Tabla 3: CONFIGURACIÓN ROUTER 1.

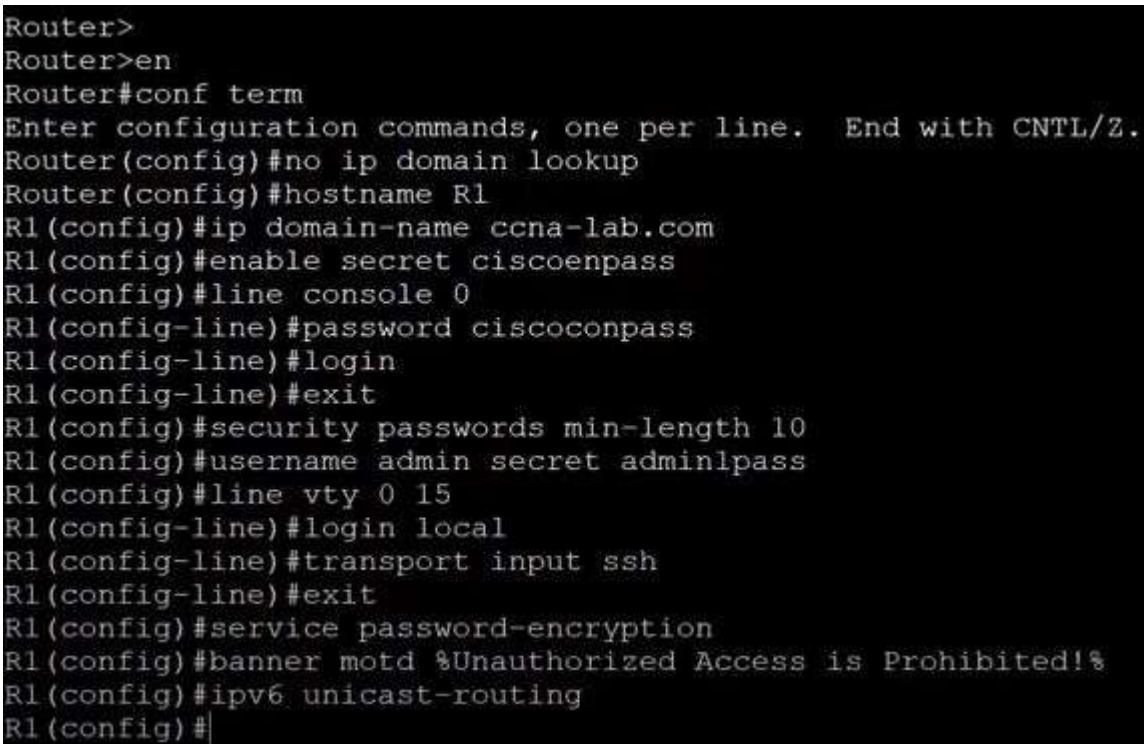

Figura 3: Configuración del R1.

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

Tabla 4: CONFIGURACIÓN INTERFACES ROUTER 1.

Paso 2: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S1 Hostname S2
Nombre de dominio	**ccna-lab.com** ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** Line console 0 Password ciscoconpass Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd %_____%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa mosulus 10242
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.98 255.255.255.248 Ipv6 address 2001:db8:acad:c::98/64 Ipv6 address fe80::98 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Ip Default-gateway 10.19.8.97

Tabla 5: CONFIGURACIÓN SWITCH 1.

S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde

Paso 3: Configure S1 y S2. – minuto 25-58

Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	No ip domain lookup
Nombre del switch	**S1 o S2, según proceda** Hostname S2
Nombre de dominio	**ccna-lab.com** ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** Enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** Line console 0 Password ciscoconpass Login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** Username admin secret admin1pass

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Line vty 0 15 Login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Transport input ssh
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Configurar un MOTD Banner	Banner motd %_____%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** Crypto key generate rsa modulus 1024 -- no soportado Crypto key generate rsa 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 Int vlan 4 Ip address 10.19.8.99 255.255.255.248 Ipv6 address 2001:db8:acad:c::99/64 Ipv6 address fe80::99 link-local Description MANAGEMENT No shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 Ip Default-gateway 10.19.8.97

Tabla 6: CONFIGURACIÓN SWITCH 2.

S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native Vlan 2 Name bikes Vlan 3 Name trikes Vlan 4 Name management Vlan 5 Name parking Vlan 6 Name native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 Interfaces G1/0/1, G1/0/2 y G1/0/5 Interface G1/0/5 Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6 Inteface range G1/0/1-2 Shutdown Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Channel-group 1 mode active Int port channel 1 Switchport trunk encapsulation dot1q Switchport mode trunk Switchport trunk native vlan 6

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 Interface g1/0/6 Switchport mode access Switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC Switchport port-security máximum 3

Tarea	Especificación
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Int range g1/0/3-4 Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown Int range g1/0/7-24 Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown Int range g1/1/1-4 Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown

Tabla 7: CONFIGURACIÓN SWITCH 1 - *(VLAN, Trunking, EtherChannel)*.

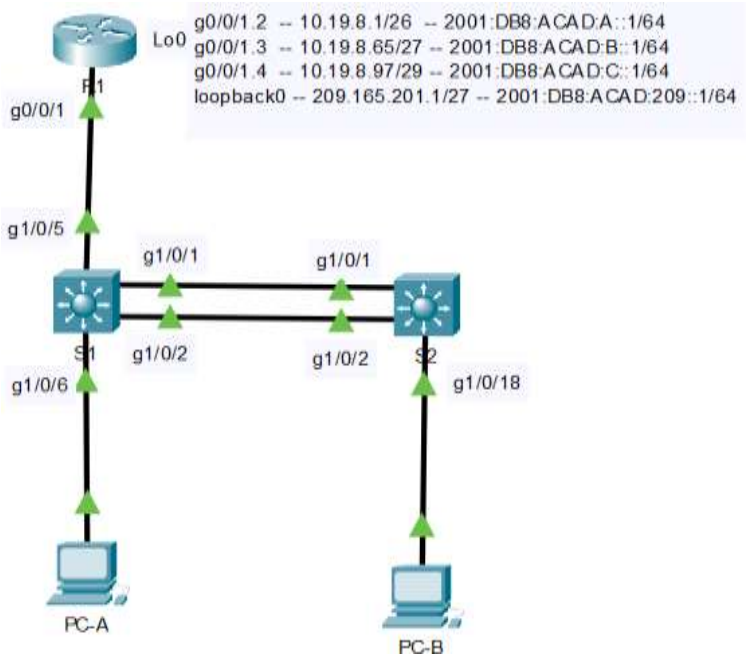

Figura 4: Configuración del S1.

Paso 5: Configure el S2.

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

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native Vlan 2 Name bikes Vlan 3 Name trikes Vlan 4 Name management Vlan 5 Name parking Vlan 6 Name native

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 Interfaces G1/0/1 y G1/0/2 Interfaces range G1/0/1-2 shutdown switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Channel-group 1 mode active Int port channel 1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 Int g0/1/18 Switchport mode Access Switchport Access vlan 3

Tarea	Especificación
Configure port-security en los access ports	permite 3 MAC addresses switchport port-security switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar Int range g1/0/3-17 Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown Int range g1/0/19-24 Switchport mode Access Switchport Access vlan 5 Description no esta en uso Shutdown Int range g1/1/1-4 Switchport mode Access Switchport Access vlan 5 Description no está en uso Shutdown

Tabla 8: CONFIGURACIÓN SWITCH 2 - (VLAN, Trunking, EtherChannel).

Debemos activar las interfaces del etherchannel

S2:

G1/0/1-2

NO SHUTDOWN

S2:

G1/0/1-2

NO SHUTDOWN

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 Ip route 0.0.0.0 0.0.0.0 loopback 0 Ipv6 route ::/0 loopback 0

Tarea	Especificación
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 10.19.8.0 /26 10.19.8.1 10.19.8.62 Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo. 10.19.8.1 - 10.19.8.52 estas son las que debemos restringir y solo trabajamos con las 10 que sobran. Debemos entonces crear el POOL desde: 10.19.8.52 - 10.19.8.62 Ip dhcp excluded-address 10.19.8.1 10.19.8.52 Ip dhcp POOL VLAN2-BIKES Network 10.19.8.0 255.255.255.192 Default-route 10.19.8.1 Domain-name ccna-b.net

Tarea	Especificación
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 TRIKES 10.19.8.64 /27 10.19.8.65 10.19.8.94 Debemos entonces restringir las primeras direcciones de este rango, ya que solo debemos trabajar con las 10 últimas del mismo. 10.19.8.65 - 10.19.8.84 estas son las que debemos restringir y solo trabajamos con las 10 que sobran. Debemos entonces crear el POOL desde: 10.19.8.85 - 10.19.8.94 Ip dhcp excluded-address 10.19.8.65 10.19.8.84 Ip dhcp POOL VLAN3-TRIKES Network 10.19.8.64 255.255.255.224 Default-route 10.19.8.65 Domain-name ccna-b.net

Tabla 9: CONFIGURACIÓN ROUTER 1 - loopback 0 - DHCP.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde

R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde

Paso 2: Configurar los servidores

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

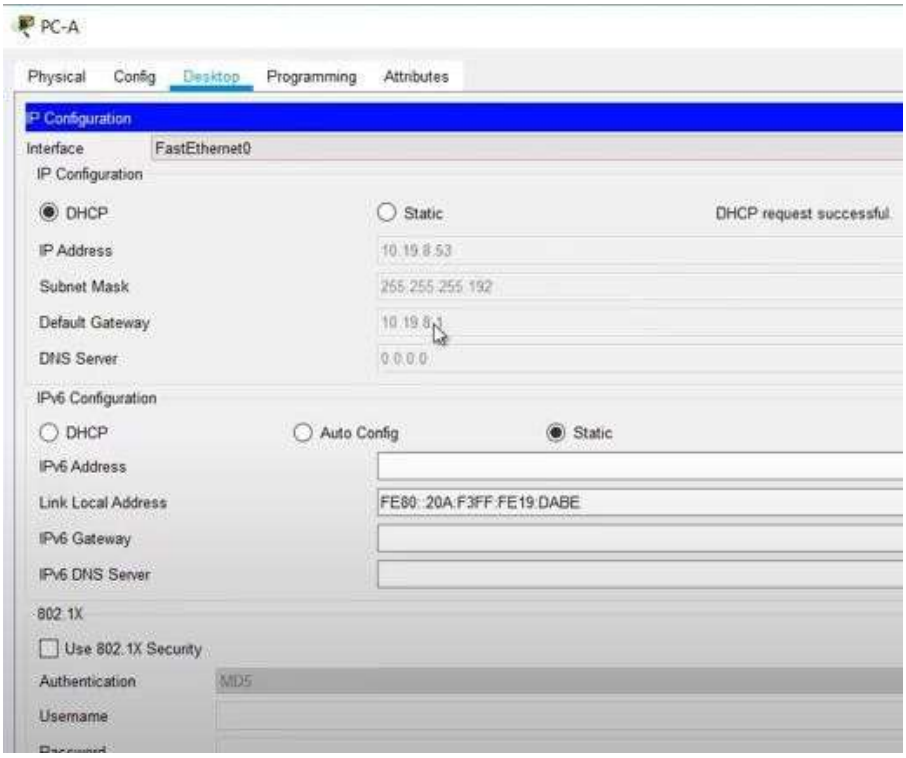

Figura 5

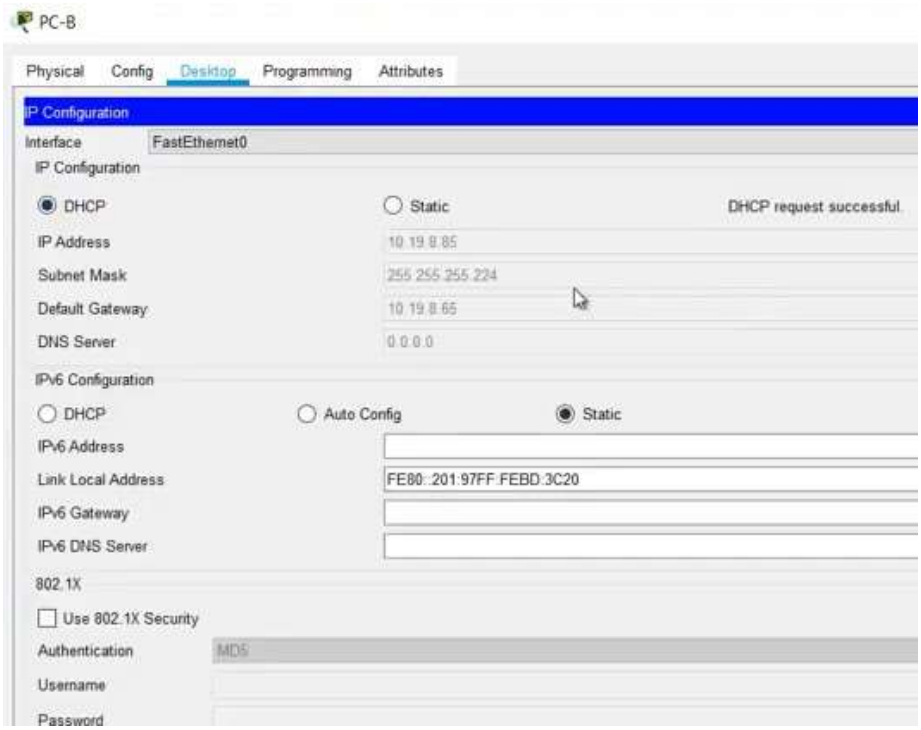
PC-B
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
DHCP request successful
IP Address
10.19.8.85
Subnet Mask
255.255.255.224
Default Gateway
10.19.8.65
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:97FF:FEBD:3C20
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password

Figura 6

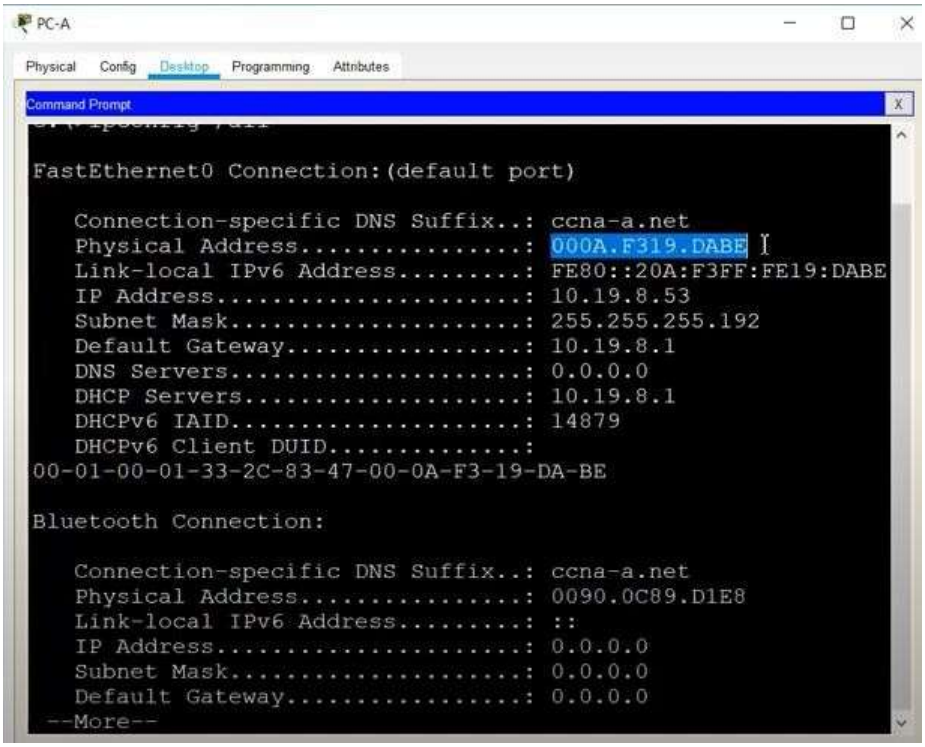

Figura 7 - verificación de DHCP en las PC.

PC-A Network Configuration	
Descripción	*PC-A*
Dirección física	
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	

Configuración de red de PC-C	
Descripción	*PC-C*
Dirección física	
Dirección IP	*10.19.8.85*

Configuración de red de PC-C	
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	

Tabla 10: CONFIGURACIÓN DHCP PC-A – PC-C

Parte 3: 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:

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
	R1, G0/0/1.3	Dirección	10.19.8.65	exitoso
		IPv6	2001:db8:acad:b: :1	exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	exitoso
		IPv6	2001:db8:acad:c: :1	exitoso
	S1, VLAN 4	Dirección	10.19.8.98	exitoso
		IPv6	2001:db8:acad:c: :98	exitoso

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

Tabla 11: Pruebas de conectividad.

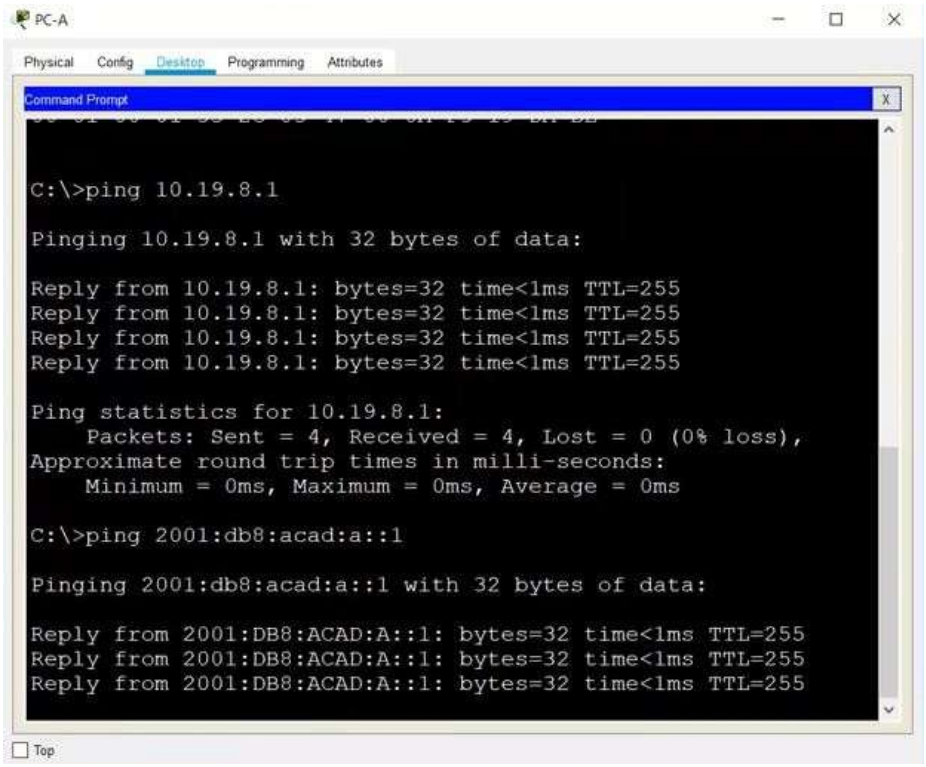

Figura 8

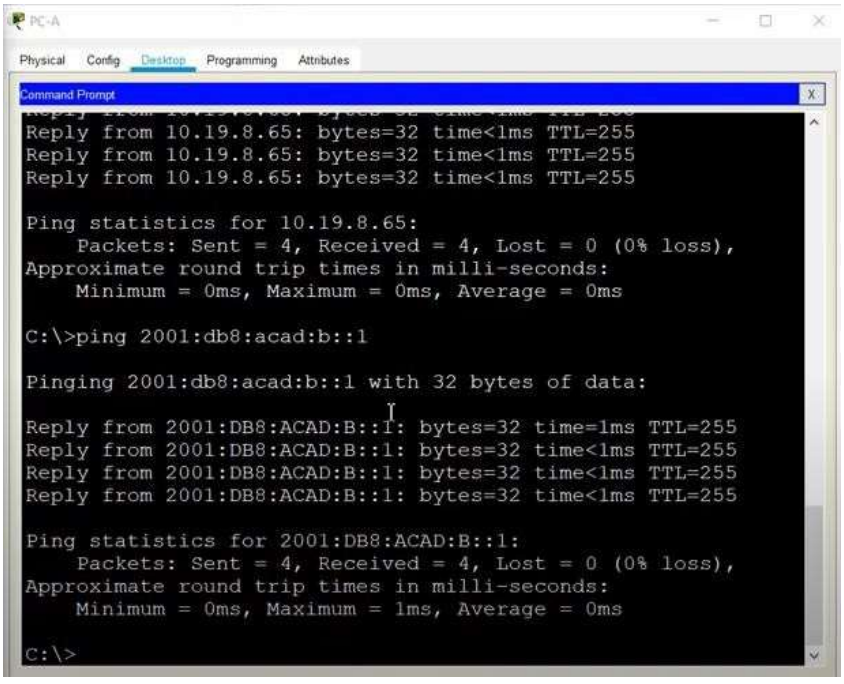

Figura 9 - pruen de conectividad desde PC-A

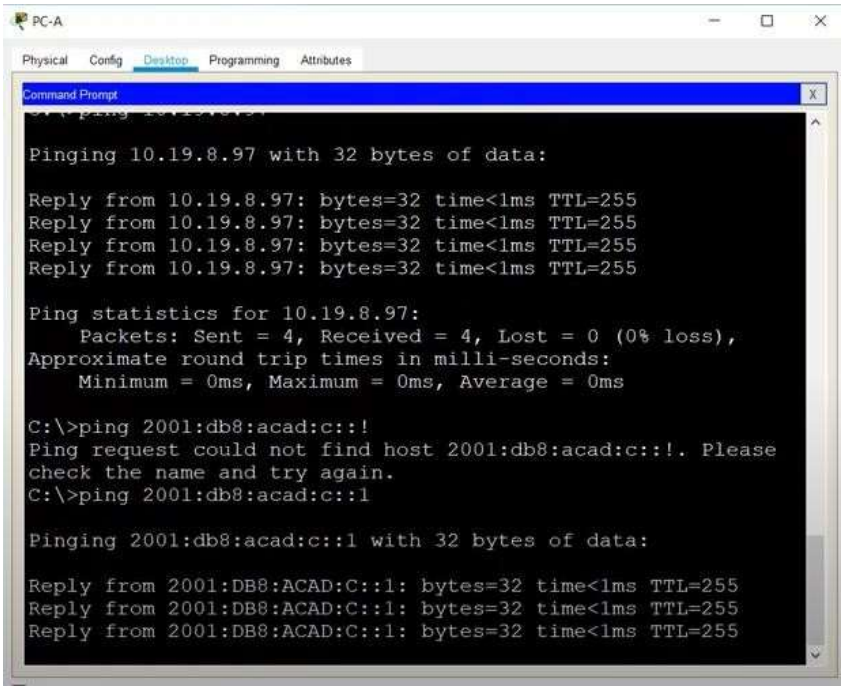

Figura 10 - pruen de conectividad desde PC-A

SWITCH 1 : no existe una puerta de enlace IPV6

Configura terminal

Ipv6 route ::/0 2001:db8:acad:c::1

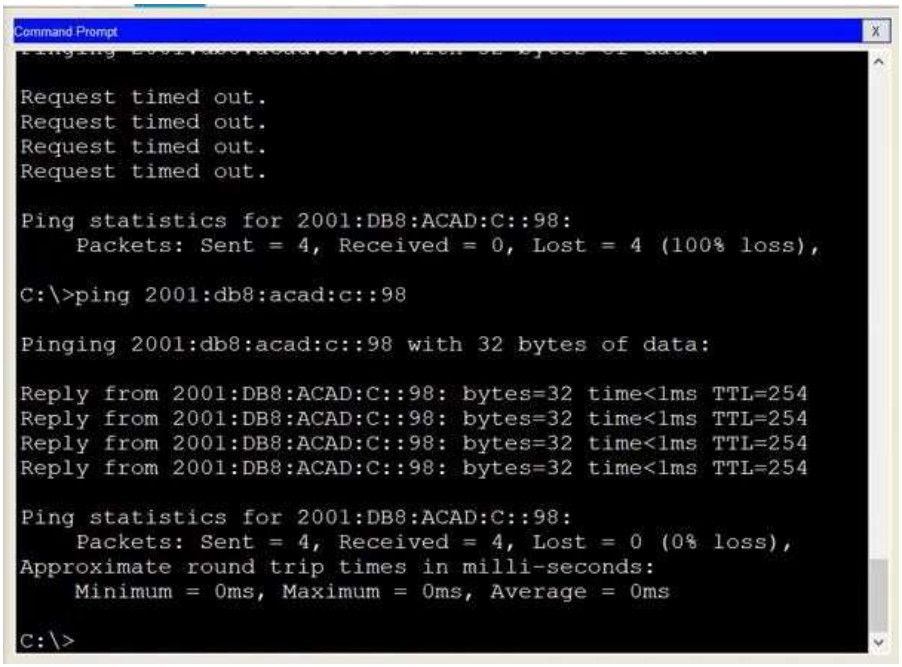

Figura 11 - Prueba puerta de enlace IPV6

SWITCH 2 : no existe una puerta de enlace IPV6

Configura terminal

Ipv6 route ::/0 2001:db8:acad:c::1

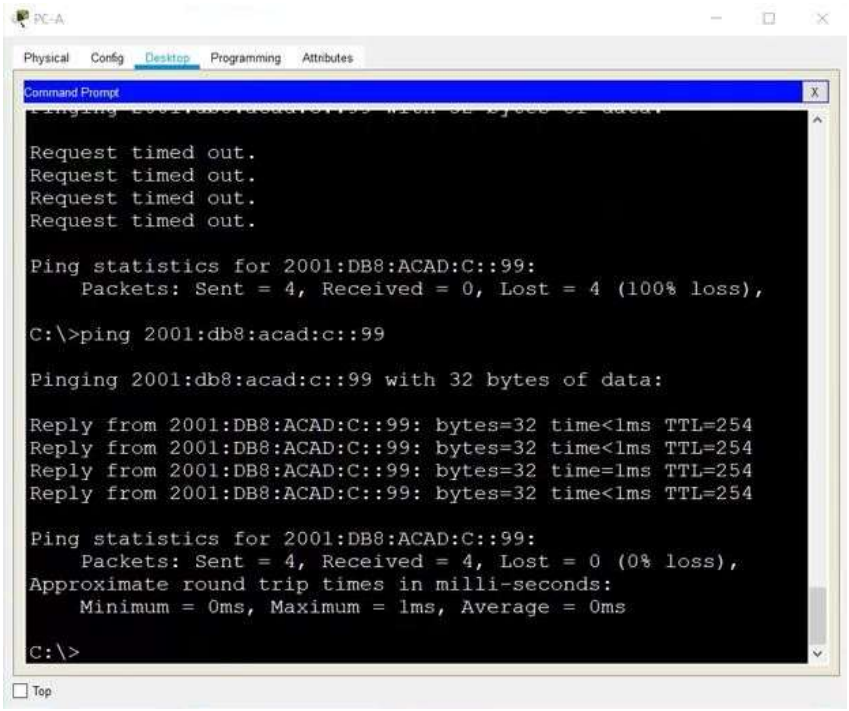
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:DB8:ACAD:C::99:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 2001:db8:acad:c::99
Pinging 2001:db8:acad:c::99 with 32 bytes of data:
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time<1ms TTL=254
Ping statistics for 2001:DB8:ACAD:C::99:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top

Figura 12

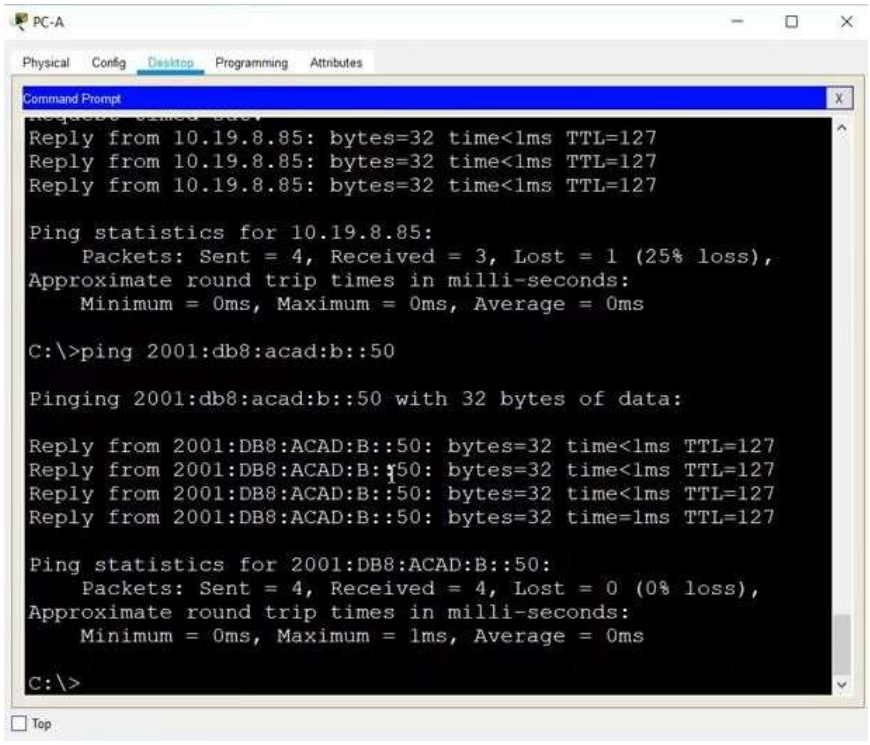
PC-A
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Reply from 10.19.8.85: bytes=32 time<1ms TTL=127
Reply from 10.19.8.85: bytes=32 time<1ms TTL=127
Reply from 10.19.8.85: bytes=32 time<1ms TTL=127
Ping statistics for 10.19.8.85:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2001:db8:acad:b::50
Pinging 2001:db8:acad:b::50 with 32 bytes of data:
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=1ms TTL=127
Ping statistics for 2001:DB8:ACAD:B::50:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top

Figura 13 - Prueba de conectividad IPV6

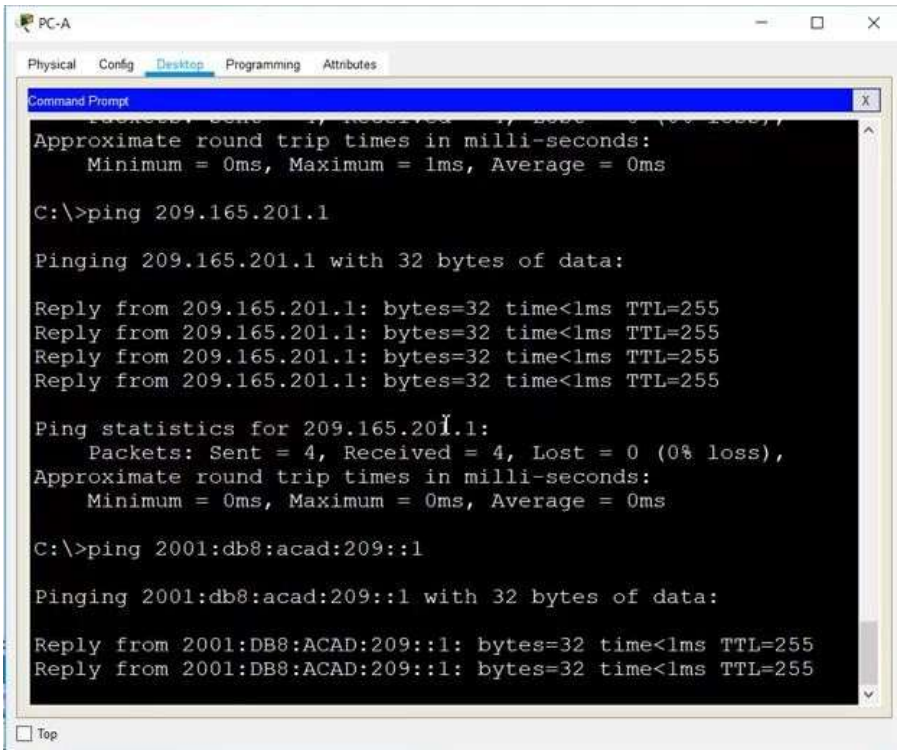

Figura 14 - Prueba de conectividad IPV6

4. ESCENARIO 2.

Escenario 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico 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

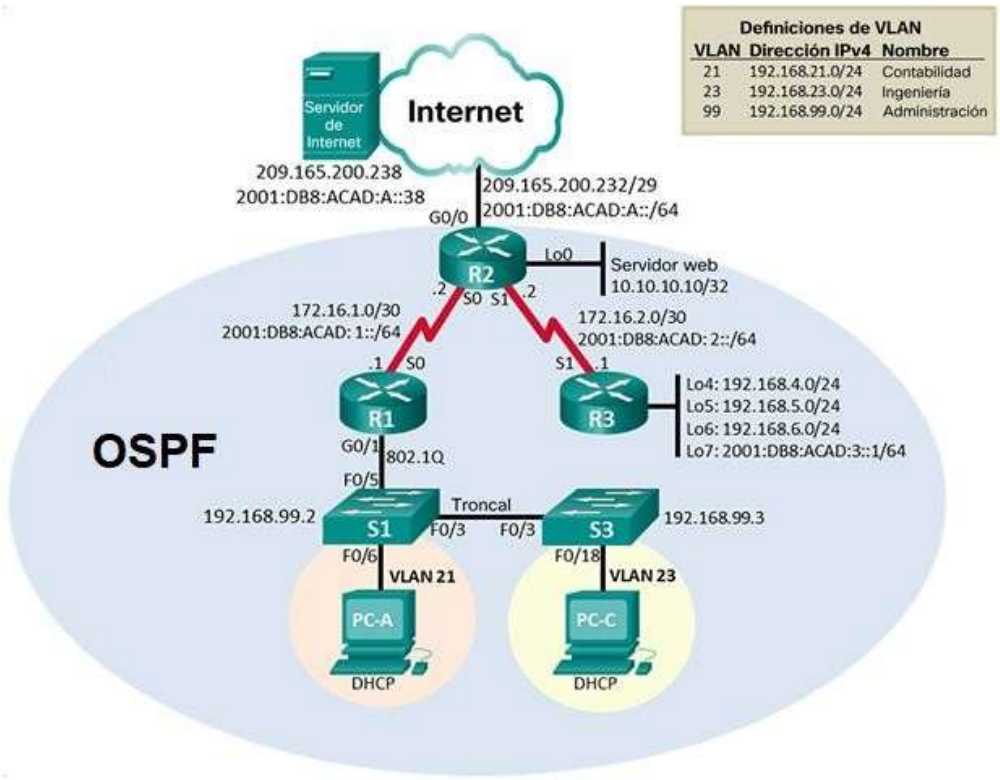

Figura 15 - TOPOLOGIA ESCENARIO 2.

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Enable Erase startup-config Reload

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

Tabla 12: reinicializar dispositivos.

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):

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 13- CONFIGURACIÓN computadora de Internet

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco

Cifrar las contraseñas de texto no cifrado	Desactivamos DNS Enable Configure terminal No ip domain lookup Hostname R1 Enable secret class Line console 0 Password cisco Login Line vty 0 15 Password cisco Login Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz Banner motd %_____% Int s 0/0/0 Descripción conexión con R2 Ip address 172.16.1.1 255.255.255.252 Ipv6 address 2001:db8:acad:1::1/64 No shutdown Clock rate 128000
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 Configurar las rutas por defecto IPV4 e IPV6 Exit Ip route 0.0.0.0 0.0.0.0 s0/0/0 Ipv6 route ::/0 s0/0/0

TABLA 14 - configuración básica R1

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookup
Nombre del router	R2 Hostname R2.
Contraseña de exec privilegiado cifrada	Class Enable secret class
Contraseña de acceso a la consola	Cisco Line console 0 Password cisco Login .
Contraseña de acceso Telnet	Cisco Line vty 0 15 Password cisco Login .
Cifrar las contraseñas de texto no cifrado	Service password-encryption .
Habilitar el servidor HTTP	Habilitamos el servidor DHCP Comando no soportado por PACKET TRACER.

Mensaje MOTD	Se prohíbe el acceso no autorizado. Commando. Banner motd % Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz Interface serial 0/0/0 Description conexión con R1 Ip address 172.16.1.2 255.255.255.252 Ipv6 addres 2001:db8:acad:1::2/64 No shutdown

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz Interface serial 0/0/1 Description conexión con R3 Ip address 172.16.2.2 255.255.255.252 Ipv6 addres 2001:db8:acad:2::2/64 Clock rate 128000 No shutdown .
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz Interface g 0/0 Description conexión a INTERNET Ip address 209.165.200.233 255.255.255.248 Ipv6 addres 2001:db8:acad:a::1/64 No shutdown .

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. Interface loopback 0 Description WEB SERVER Ip address 10.10.10.10 255.255.255.255 .
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. Ruta por defecto Ip route 0.0.0.0 0.0.0.0 g0/0 Ipv6 route ::/0 g0/0

TABLA 15 - configuración básica R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain-lookp .
Nombre del router	R3 Hostname R3
Contraseña de exec privilegiado cifrada	Class Enable secret class

Contraseña de acceso a la consola	Cisco Line console 0 Password cisco Login .
Contraseña de acceso Telnet	Cisco Line vty 0 15 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. Banner motd %_____%.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz Commando. Interface s0/0/1 Description conexión con R2 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:db8:acad:2::1/64 No shutdown

Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Int loopback 4 Ip address 192.168.4.1 255.255.255.0 .
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Int loopback 5 Ip address 192.168.5.1 255.255.255.0 .
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Int loopback 6 Ip address 192.168.6.1 255.255.255.0 .
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Int loopback 7 Ipv6 address 2001:db8:acad:3::1/64.
Rutas predeterminadas	

TABLA 16 - configuración básica R3

Ip route 0.0.0.0 0.0.0.0 s0/0/1

Ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Commando No ip domain lookup.
Nombre del switch	S1 Hostname S1.
Contraseña de exec privilegiado cifrada	Class Enable secret class .
Contraseña de acceso a la consola	Cisco Line console 0 Password cisco Login.
Contraseña de acceso Telnet	Cisco Line vty 0 15 Password cisco Login.
Cifrar las contraseñas de texto no cifrado	Service password-encryption .
Mensaje MOTD	Se prohíbe el acceso no autorizado. Banner moptd % Se prohíbe el acceso no autorizado.% .

TABLA 17 - configuración básica S1

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup .
Nombre del switch	S3 Hostname S3 .
Contraseña de exec privilegiado cifrada	Class Enable secret class .
Contraseña de acceso a la consola	Cisco Line console 0 Password cisco Login.
Contraseña de acceso Telnet	Cisco Line vty 0 15 Password cisco Login .
Cifrar las contraseñas de texto no cifrado	Service password-encryption .
Mensaje MOTD	Se prohíbe el acceso no autorizado. Banner motd % Se prohíbe el acceso no autorizado.% .

TABLA 18 - configuración básica S3

Paso 7: Verificar la conectividad de la red

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

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

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

TABLA 19 - prueba conectividad, dispositivos directos.

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican Vlan 21 Name accounting Vlan 23 Name engineering Vlan 99 Name management .
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología Interface vlan 99 Ip address 192.168.99.2 255.255.255.0 N o shutdown .
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ip default-gateway 192.168.99.1 .

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Int f 0/3 Switchport mode trunk Switchport trunk native vlan 1 .
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa Int f 0/5 Switchport mode trunk Switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Int range f0/1-2, f0/4, f0/6-24, g0/1-2 Switchport mode access
Asignar F0/6 a la VLAN 21	Int f 0/6 Switch port acces vlan 21
Apagar todos los puertos sin usar	Int range f0/1-2, f0/4, f0/7-24, g0/1-2 Shutdown

TABLA 19 - S1 – vlans, interfaces, enlaces trunk

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. Vlan 21 Name accounting Vlan 23 Name engineering Vlan 99 Name management .
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología Interface vlan 99 Ip address 192.168.99.3 255.255.255.0 No shutdown .

Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. Ip default-gateway 192.168.99.1 .
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa Int f 0/3 Switchport mode trunk Switchport trunk native vlan 1 .
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range Int range f0/1-2, f0/4-24, g0/1-2 Switchport mode access .
Asignar F0/18 a la VLAN 21	Int f0/18 Siwtchport Access vlan 23 .
Apagar todos los puertos sin usar	Int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 Shutdown.

TABLA 20 - S3 – vlans, interfaces, enlaces trunk

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz Int g0/1.21 Description VLAN 21 Encapsulation dot1q 21 Ip address 192.168.21.1 255.255.255.0 .
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz Int g0/1.23 Description VLAN 23 Encapsulation dot1q 23 Ip address 192.168.23.1 255.255.255.0 .

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz Int g0/1.99 Description VLAN 99 Encapsulation dot1q 99 Ip address 192.168.99.1 255.255.255.0 .
Activar la interfaz G0/1	Exit Int g0/1 No shutdown .

TABLA 21 - R1 – configuración vlans, interfaces.

Paso 4: Verificar la conectividad de la red

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

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

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

TABLA 22 prueba de conectividad.

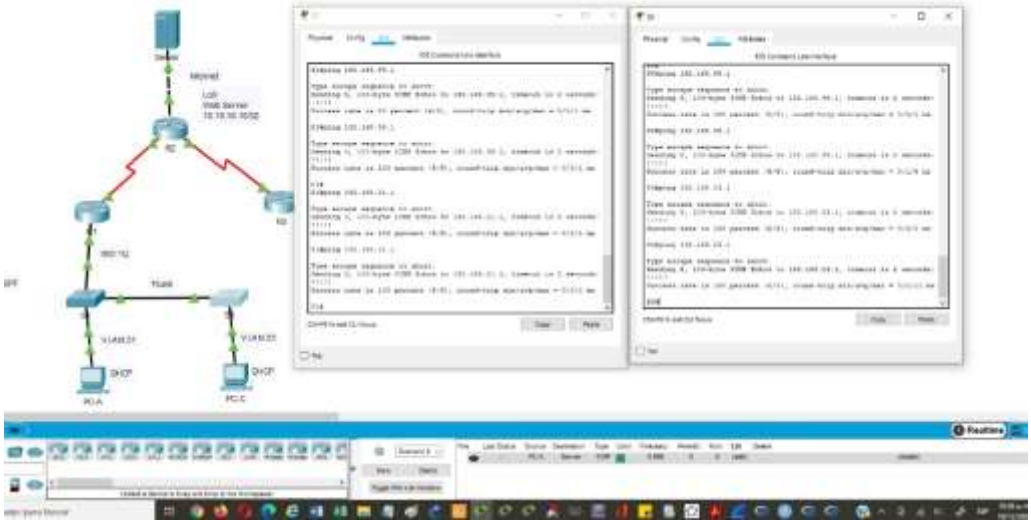

Figura 16 - prueba de conectividad S1 Y S2.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Commando. router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0.

Establecer todas las interfaces LAN como pasivas	*passive-interface GigabitEthernet0/1.21* *passive-interface GigabitEthernet0/1.23* *passive-interface GigabitEthernet0/1.99* .
Desactive la sumarización automática	No auto-summary.

TABLA 23 Configurar OSPF R1.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1.
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. network 10.10.10.10 0.0.0.0 area 0 network 172.16.1.0 0.0.0.3 area 0 network 172.16.2.0 0.0.0.3 area 0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface Loopback0.
Desactive la sumarización automática.	No auto summary.

TABLA 24 Configurar OSPF R2.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1.

Anunciar redes IPv4 conectadas directamente	network 172.16.2.0 0.0.0.3 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0.
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface Loopback4 passive-interface Loopback5 passive-interface Loopback6.
Desactive la sumarización automática.	No auto-summary.

TABLA 25 Configurar OSPF R3.

Paso 4: Verificar la información de OSPF

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

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	*Show protocols Commando.*

Figura 17 - show protocols R1.

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

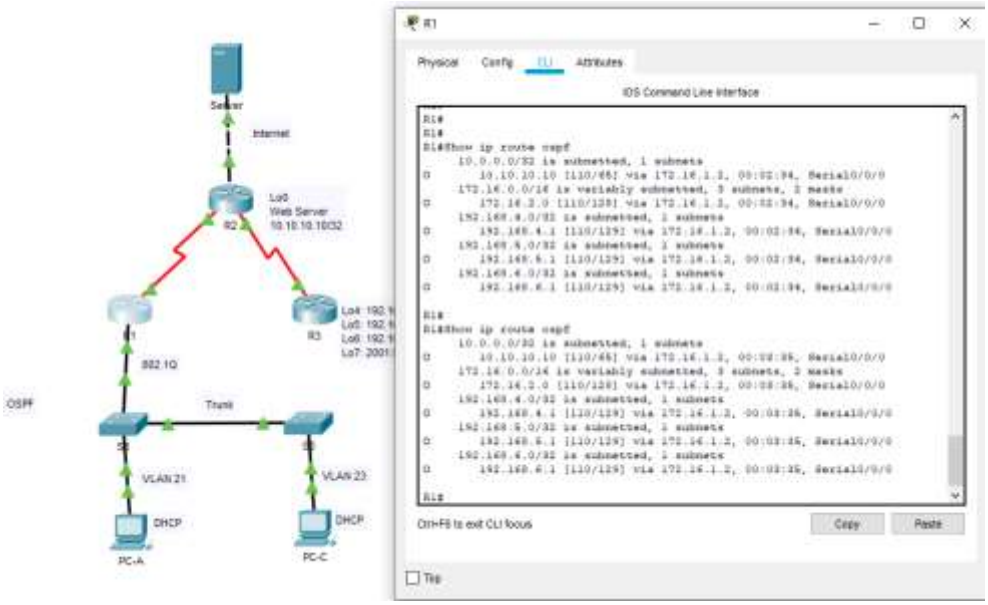

Figura 18 - show ip route ospf en R1

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

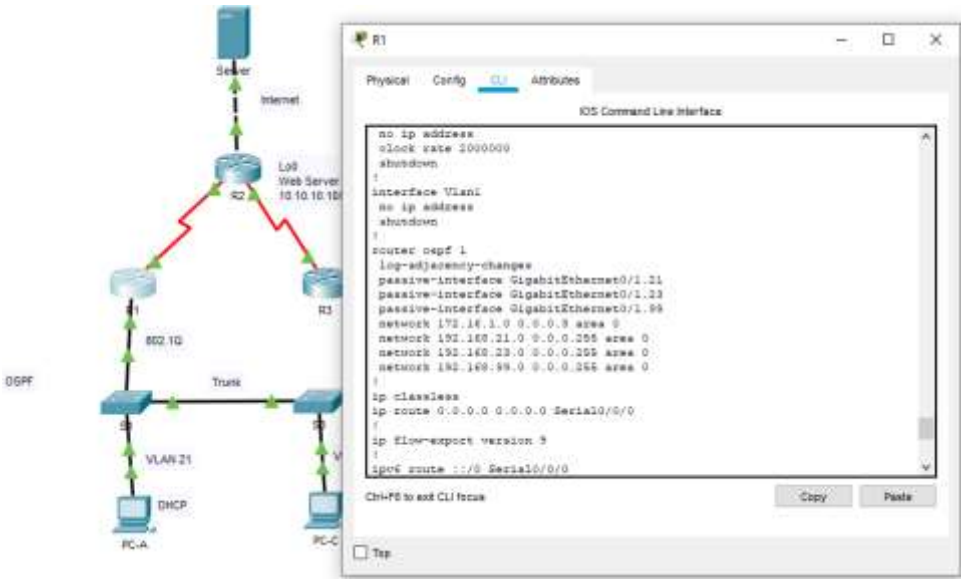

Figura 19 - show running-config en R1

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20.
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20 .
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10.
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 .

TABLA 26 - Configurar el R1 como servidor de DHCP

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

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** username webuser privilege 15 secret 5 cisco12345.
Habilitar el servicio del servidor HTTP	ip http server.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local.
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** ip nat inside source static 10.10.10.10 209.165.200.237.
Asignar la interfaz interna y externa para la NAT estática	interface GigabitEthernet0/0 ip nat outside.

Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255.
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228 ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248.
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET.

TABLA 27 - Configurar la NAT estática y dinámica EN R2

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Exitoso*
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.	*Exitoso*

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**	*En packet tracer muestra un mensaje de error, posible al 100% en laboratorio real*

TABLA 28 - verificación de DHCP y NAT.

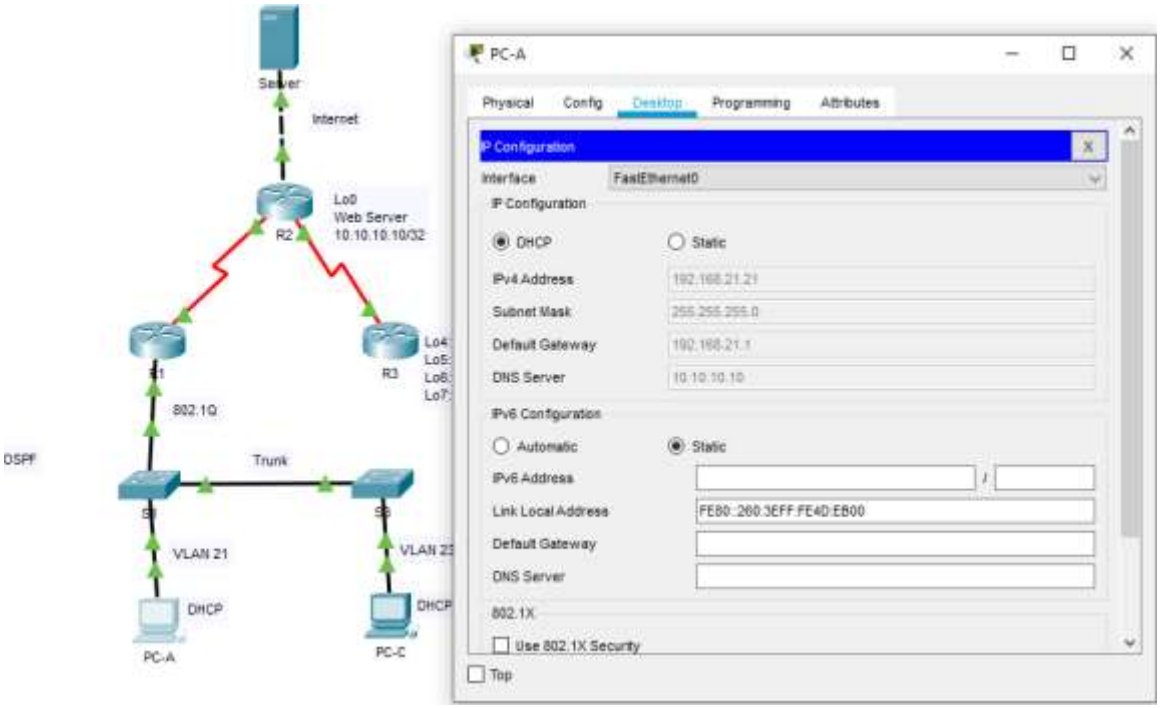

Figura 20 - verificación DHCP en PC-A.

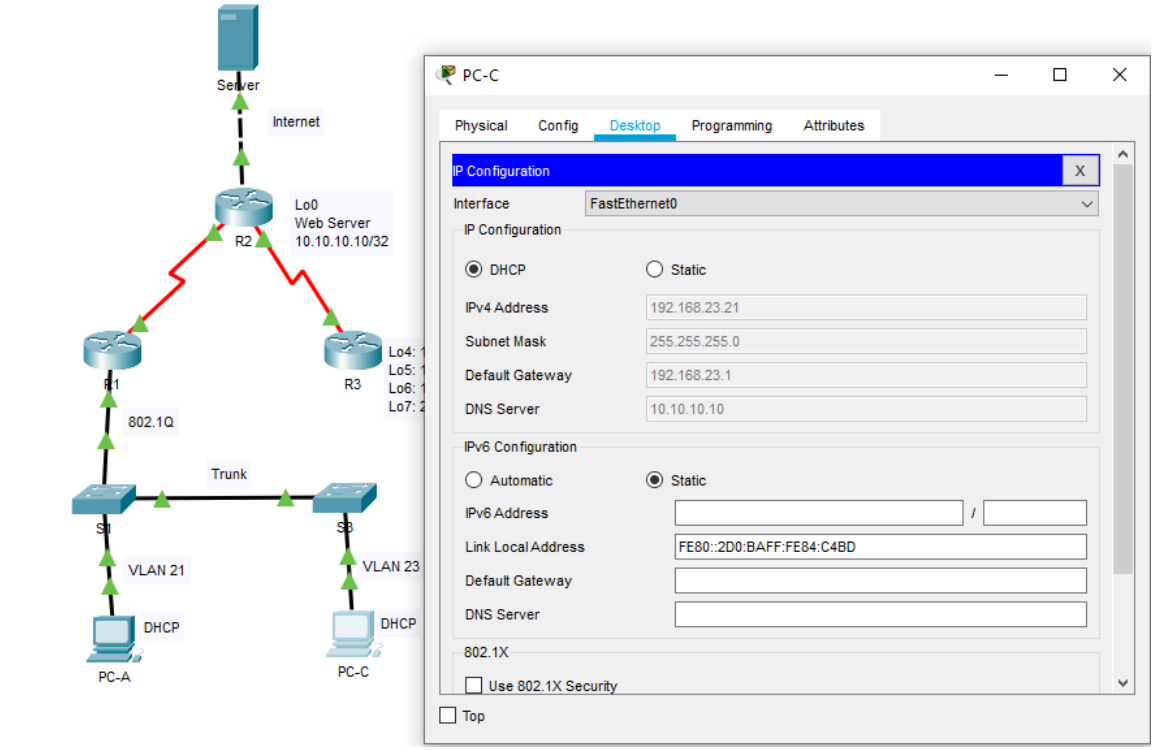

Figura 21 - verificación DHCP en PC-C.

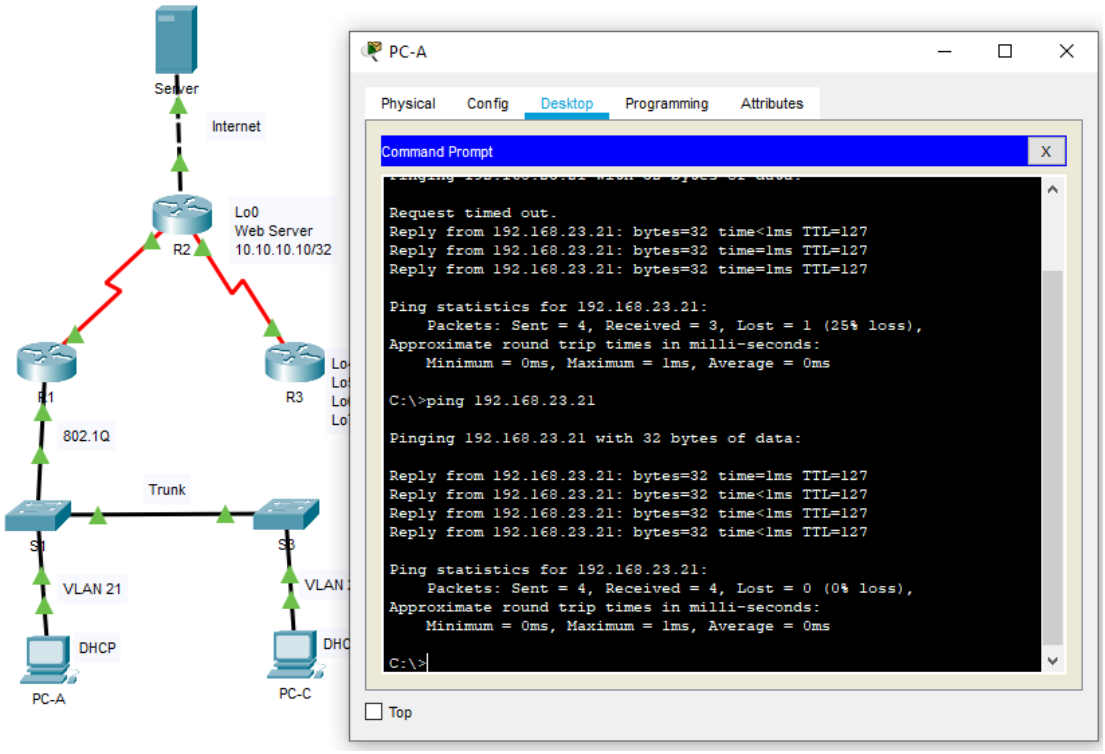

Figura 22 - PING desde PC-A.

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** clock set 09:00:00 5 March 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** ntp manster 5

Configurar R1 como un cliente NTP.	Servidor: **R2** ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	ntp update-calendar
Verifique la configuración de NTP en R1.	show ntp status.

TABLA 29 - Configuración de NTP.

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

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

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** ip access-list standard ADMIN-MGT permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in .
Permitir acceso por Telnet a las líneas de VTY	line vty 0 4 transport input telnet.
Verificar que la ACL funcione como se espera	show access-list.

TABLA 30 - Configuración de restrocciones en R2.

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	*Show ip access-list*
Restablecer los contadores de una lista de acceso	*Clear access-list counters*
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	*Show ip interface s0/0/0*
¿Con qué comando se muestran las traducciones NAT?	*Show ip nat translation* ***Nota:*** *Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.*
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	*Clear ip nat translation **

TABLA 31 - Comandos CLI.

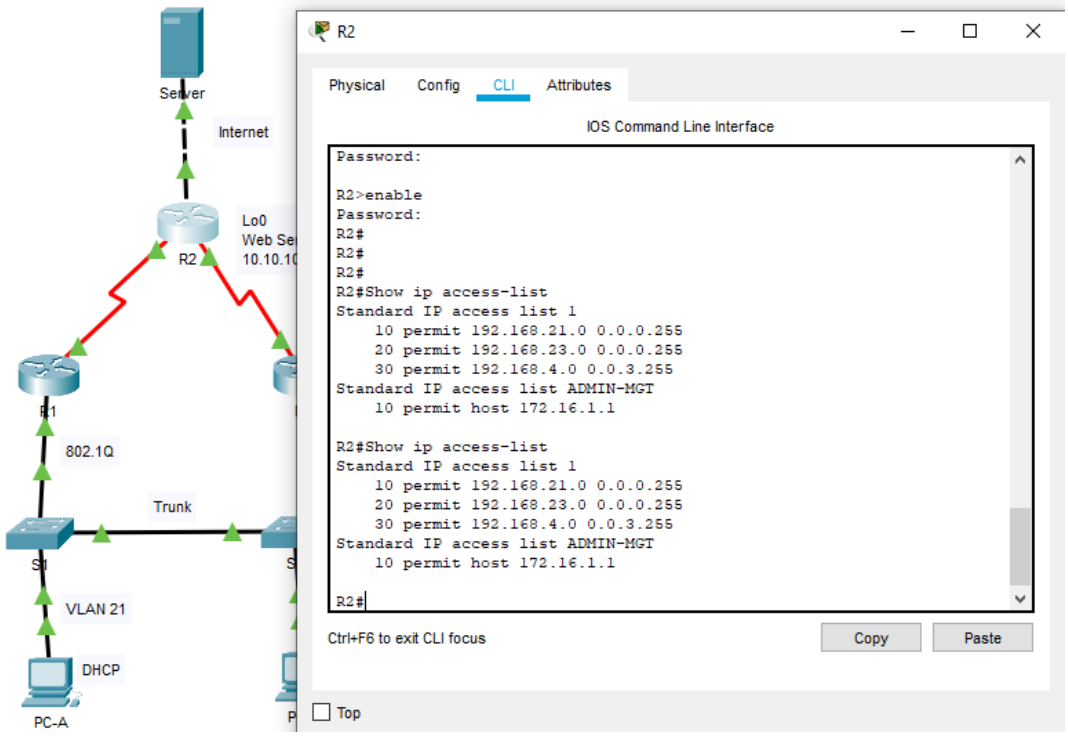

Figura 23 - verificación de ACL EN R2

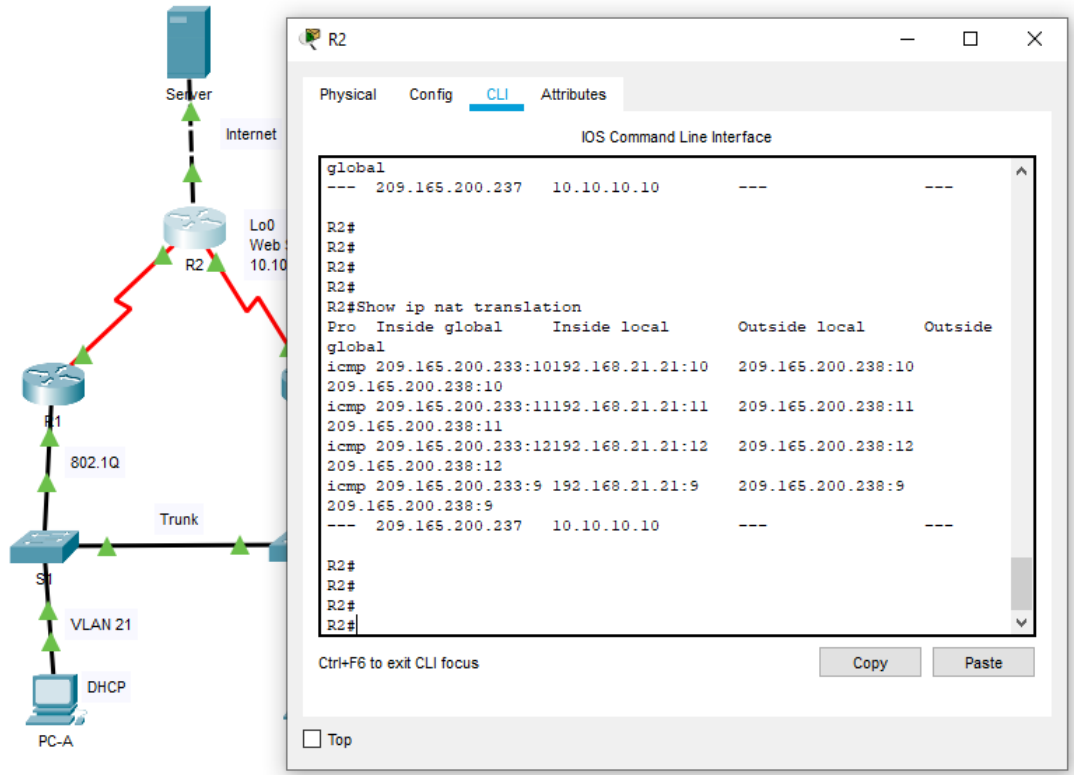

Figura 24 - verificación NAT en R2.

ARTICULO CIENTIFICO

https://drive.google.com/file/d/16y1MR1iVSfW8izL2yndzztmWx4gAEbGb/view?usp=sharing

PING Y TRACEROUTE.

Aplico este comando con el fin de verificar que tal está funcionando nuestra red en lo que tiene que ver con la conectividad, además estos comandos son muy útiles a la hora de solucionar algún tipo de inconveniente.

Vemos que todos los puntos de la red están respondiendo, con esto concluimos que todo el proceso de diseño y montaje de la red está bien elaborado.

SIMULADOR.

Cada uno de estos comandos ya han sido verificados en la comprobación de cada paso.

CONCLUSIONES

- De acuerdo a todo lo realizado en este trabajo podemos concluir que la topología implementada del curso de profundización de cisco es una herramienta útil para mi futuro profesional demostrando que se cumplió con todos los objetivos propuestos para el desarrollo de este.
- Utilizamos VLSM con el fin de que el desperdicio de direcciones IP sea mucho menor y podamos ajustar las subredes a las necesidades reales de cada una de ellas.
- Con la utilización de la herramienta de simulación de redes Packet Tracer podemos trasladarnos a la realidad para la elaboración de redes con la cual optimizamos tiempo y dinero para la construcción de redes.
- Nos practicamos mucho con los comandos para verificación de conexión como los ping, tracert, y muchos otros mas, los cuales nos facilitan la tarea de verificación.

BIBLIOGRAFIA Y WEBGRAFIA

Tomado de: http://www.ipv6go.net/lte/

Tomado de: http://informatica.uv.es/iiguia/2000/AER/Practica5.pdf

BIBLIOGRAFIA

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