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

WILFER VELEZ OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E NGENIERIAS ECBTI
INGENIERIA DE TELECOMUNICACIONES
CALI
2020

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

WILFER VELEZ OROZCO

Diplomado de opción de grado presentado para optar el título de INGENIERO DE TELECOMUNICACIONES

TUTOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E NGENIERIAS ECBTI
INGENIERIA DE TELECOMUNICACIONES
CALI
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

DHCP: DHCP significa protocolo de configuración de host dinámico y es un protocolo de red utilizado en redes IP donde un servidor DHCP asigna automáticamente una dirección IP y otra información a cada host en la red para que puedan comunicarse de manera eficiente con otros puntos finales.

VLAN: Una V LAN (Virtual LAN) agrupa lógicamente dispositivos en un mismo dominio de broadcast, creando lógicamente distintas redes como si fueran distintas redes físicas.

Usualmente una VLAN se configura en un switch para agrupar interfaces físicas en un mismo dominio de broadcast y otras VLANs con otras interfaces en otros grupos de interfaces físicas. Incluso se puede configurar la misma VLAN en distintos switches.

OSPF: Open Shortest Path First (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). OSPF es un protocolo de pasarela interior (IGP).

NAT: La conversión de direcciones de red (NAT) permite acceder a Internet de una forma segura y sin tener que cambiar las direcciones IP de la red privada.

Las empresas utilizan redes privadas, lo que les permite seleccionar las direcciones IP que deseen. Sin embargo, si dos empresas tienen direcciones IP duplicadas e intentan comunicarse entre sí, tendrán problemas. Para poder comunicarse en Internet, es necesario tener una dirección publica y registrada. Como su nombre indica, NAT es un mecanismo que convierte una dirección privada en publica.

ACL: Una Lista de Control de Accesos (ACL: Access Control List) es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de estos.

RESUMEN

En la actualidad las telecomunicaciones están representando un gran desafío tanto paras las compañías antiguas que deben mantenerse a la vanguardia en términos de tecnología como también para aquellas nacientes las cuales se enfrentan a un mercado altamente copado y en el cual aquellos que logren sacar el máximo provecho de los recursos tecnológicos tendrá igualmente grandes posibilidades de triunfar, esto anterior no aplica solo en el entorno empresaria sino también para temas médicos, educativos, militares y políticos.

De acuerdo con lo anterior se hace necesario que cada profesional en el área de las telecomunicaciones este en capacidad de analizar los requerimientos técnicos planteados en cada escenario hipotético o real y basado en los conocimientos adquiridos durante el programa académico presentar una solución integral ya sea a través de herramientas de virtualización como Packet Tracer o implementándolo en equipos reales.

En el presente documento se abordarán específicamente dos escenarios en los cuales podremos visualizar la metodología aplicada para la implementación y puesta en marcha de conceptos como DHCP, VLAN, OSPF, NAT, ACL, NTP, EtherChannel entre otros que serán vistos con mayor detalle a continuación.

ABSTRACT

At present telecommunications are representing a great challenge both for old companies that must stay at the forefront in terms of technology as well as for those nascent which face a highly crowded market and in which those who manage to get the most out of it. of technological resources will have equally great possibilities of success, this above not only applies in the business environment but also for medical, educational, military and political issues.

In accordance with the foregoing, it is necessary for each professional in the telecommunications area to be able to analyze the technical requirements raised in each hypothetical or real scenario and based on the knowledge acquired during the academic program, present a comprehensive solution either through virtualization tools such as Packet Tracer or implementing it on real computers.

In this document, two scenarios will be specifically addressed in which we will be able to visualize the methodology applied for the implementation and start-up of concepts such as DHCP, VLAN, OSPF, NAT, ACL, NTP, EtherChannel, among others that will be seen in greater detail below. .

OBJETIVOS

Por medio del desarrollo de estos dos escenarios se espera presentar claramente el proceso por medio del cual se implementaras dos diseños red diferentes en los cuales se abordarán diferentes configuraciones con el fin de logar conectividad en ellos.

En el escenario número 1 se espera dar conectividad a dos switch los cuales deberán manejar diferentes VLAN e igualmente tener la capacidad de operar entre ellos por medio una canal EtherChannel, así mismo se deberá tener puertos de acceso y troncales para con el fin de permitir tráfico entre las diferentes VLAN.

En este mismo escenario tendremos un Router quien se deberá encargar de la gestión del enrutamiento entre VLANs al igual que prestar el servicio de servidor de DHCP

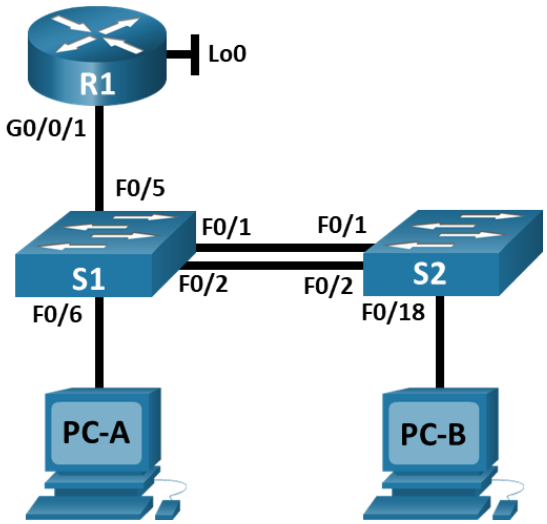
En el escenario 2 se planteará un diseño de red un poco más complejo en el cual se deberá interactuar con una red de tres Router, dos Switch, dos PC y un servidor que simulará ser un servicio web en Internet.

Durante este desarrollo de deberán implementar diferentes servicios como el protocolo de enrutamiento OSPF, servicio de DHCP para dos VLAN diferentes, NAT estático y dinámico para simular conexión a internet con una única dirección IPV4 publica o también asignando un Pool de direcciones, también se deberá hacer restricción de tráfico por medio de ACLs y por último se espera que se configure uno de los routers como servidor NTP y otro como cliente.

DESARROLLO

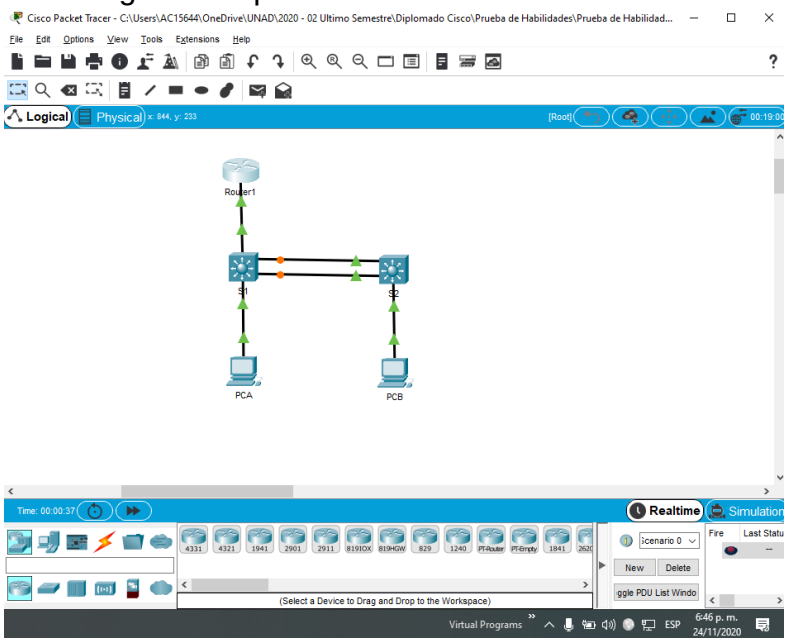
ESCENARIO 1

Figura 1 Topología escenario # 1



Fuente: UNAD

Figura 2 Implementación en Packet Tracer



Fuente: Autor

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos.

A continuación, se realiza el proceso inicial en los SW y Routers, Como el desarrollo de esta prueba de habilidades se está desplegando en Packet Tracer los dispositivos ya se encuentran en estado de fábrica,

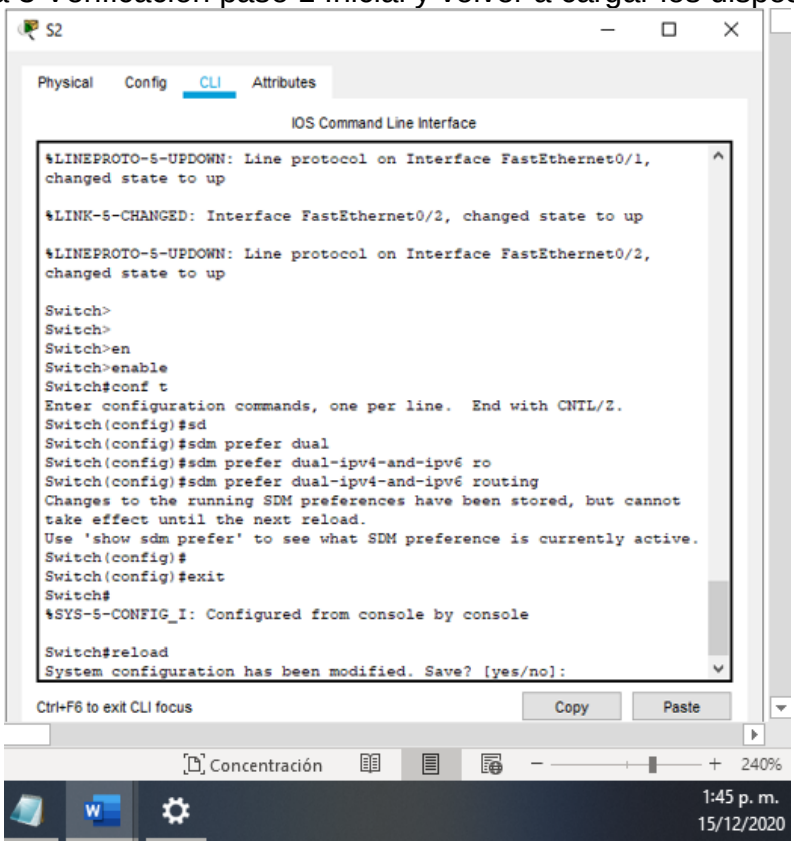
Paso1: Inicializar y volver a cargar el router y el switch

Tabla 1 Inicializar y volver a cargar el router y el switch

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch#RELOAD
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash:
Configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch	Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing Switch#reload

A continuación, en la siguiente figura podremos evidenciar el proceso descrito en la tabla anterior donde se reinicia el S2 y se aplica la plantilla SDM para permitir comando IPV6

Figura 3 Verificación paso 1 Inicial y volver a cargar los dispositivos



Fuente: Autor

En esta parte inicial veremos cómo se aplica la configuración básica al Router 1, primero se desactiva la búsqueda de DNS, luego reemplazo el nombre del dispositivo para poderlo identificar fácilmente, asigno un nombre de dominio y luego se configuran los parámetros de seguridad tanto para la conexión por consola como para el acceso remoto por medio de las líneas VTY, también coloco el comando que permite realizar la encriptación de todas las contraseñas, por ultimo establezco un mensaje de alerta que para todos aquellos que tengan intención de conectarse al dispositivo sean notificados con algún mensaje de interés, finalmente habilito el enrutamiento IPV6.

En la segunda etapa de este paso 1, realizo la configuración IP de la interfaz Giga Ethernet con sus respectivas subinterfaces y adicionalmente habilito una interfaz loopback con direccionamiento tanto IPV4 como IPV6.

Tabla 2 Configurar R1

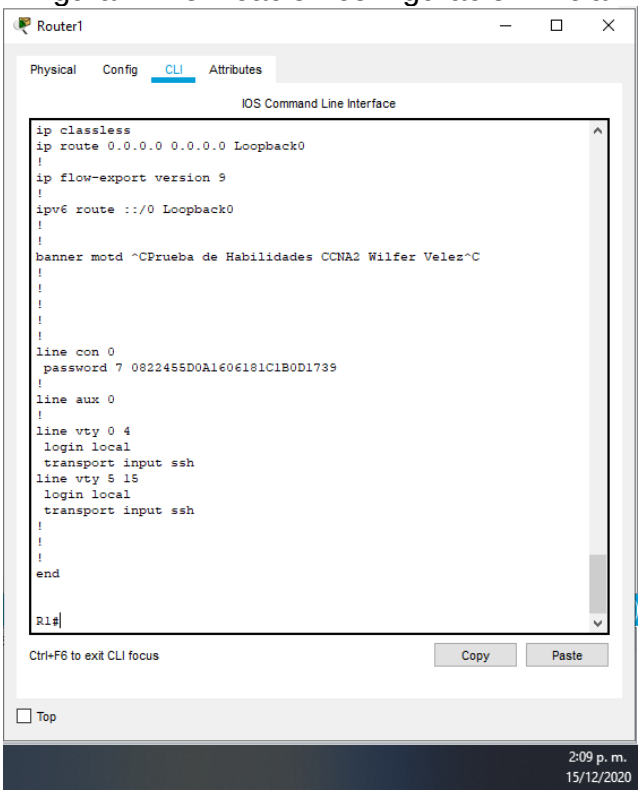
Tarea	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	ccna-lab.com R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	10 caracteres R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Prueba de Habilidades CCNA2 Wilfer Velez"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción R1(config-subif)#description Subinterface VLAN 2 BIKES Establece la dirección IPv4. R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 Establezca la dirección local de enlace IPv6 como **fe80: :1** R1(config-subif)#ipv6 address fe80::1 link-local Establece la dirección IPv6. R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz. R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	Establezca la descripción R1(config)#interface loopback 0 R1(config-if)# R1(config-if)#description Loopback0 Establece la dirección IPv4. R1(config-if)#ip address 209.165.201.1 255.255.255.224 Establece la dirección IPv6. R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 Establezca la dirección local de enlace IPv6 como **fe80::1** R1(config-if)#ipv6 address fe80::1 link-local

Tarea	Especificación
Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

En la siguiente figura se puede evidenciar la configuración aplicada sobre el Router 1 en la cual vemos el banner y los parámetros de seguridad aplicados sobre las líneas de consola y VTY

Figura 4. Verificación configuración inicial



Fuente autor

A continuación realizo la configuración básica de seguridad en los Switch 1 y 2, primero desactivo la búsqueda de DNS, luego reemplazo el nombre del dispositivo para poderlo identificar fácilmente, asigno un nombre de dominio y luego se configuran los parámetros de seguridad tanto para la conexión por consola como para el acceso remoto por medio de las líneas VTY, también coloco el comando que permite realizar la encriptación de todas las contraseñas, por ultimo establezco un mensaje de alerta que para todos aquellos que tengan intención de conectarse al dispositivo.

En la segunda etapa realizo la configuración IP de la SVI en IPV4 e IPV6 esto permitirá tener administración remota de los Swtch, finalmente configure la ruta por defecto para los dos equipos, esta ruta por defecto será la dirección IP del Router 1.

Tabla 3 Configurar S1 y S2.

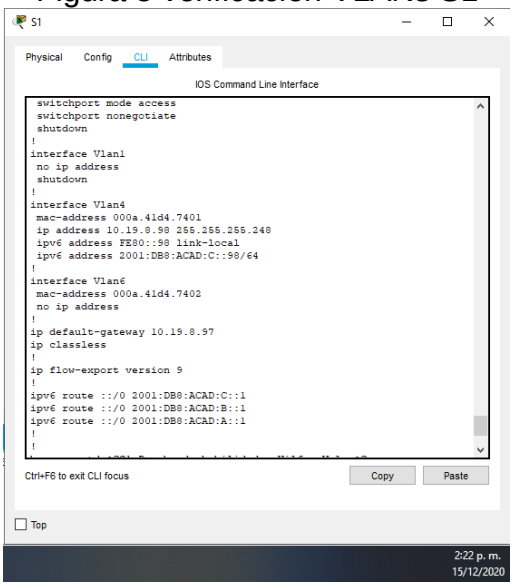
Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup Switch0(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S1 Switch0(config)#hostname S2
Nombre de dominio	**ccna-lab.com** S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** S1(config)#enable secret ciscoenpass S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass

Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd "S1 Prueba de habilidades Wilfer Velez" S2(config)#banner motd "S2 Prueba de habilidades Wilfer Velez"
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#CRYpto key generate rsa How many bits in the modulus [512]: 1024

Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S2(config-if)#ip address 10.19.8.99 255.255.255.248 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1** S1(config-if)#ipv6 address FE80::98 link-local S2(config-if)#ipv6 address FE80::99 link-local **y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)#ip default-gateway 10.19.8.97 S2(config)#ip default-gateway 10.19.8.97

En la siguiente figura se evidencia la configuración aplicada sobre el SW1 en el cual nos solicitaban aplicar la configuración IP para la Vlan de administración y el Default Gateway

Figura 5 verificación VLANs S1



Fuente. Autor

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

En la parte 2 de este escenario 1 implementé las VLAN que se definieron en el ejercicio, además configuré puertos troncales para permitir el tránsito de varias VLAN, también habilité un EtherChannel con el fin de utilizar dos interfaces físicas en la interconexión de los Switch, se les dio seguridad a los puertos de los dispositivos permitiendo máximo 3 direcciones MAC por cada uno.

Finalmente apliqué un estándar para los puertos no utilizados (Modo Acceso, Descripción y ShutDown.)

Tabla 4 Configurar en S1

Tarea	**Especificación**
Crear VLAN	VLAN 2, nombre Bikes S1(config-vlan)#name Bikes VLAN 3, nombre Trikes S1(config-vlan)#name Trikes VLAN 4, name Management S1(config-vlan)#name Management VLAN 5, nombre Parking S1(config-vlan)#name Parking VLAN 6, nombre Native S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#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 S1(config-if)#channel-group 1 mode active S1(config-if)#channel-protocol lacp
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#interface range FAstEthernet 0/3-4 , fastEthernet 0/7 - 24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Interfaces no utlizadas S1(config-if-range)#sh

En esta siguiente etapa se realiza el mismo procedimiento descrito en la tabla 3 pero en este caso sobre el Switch 2

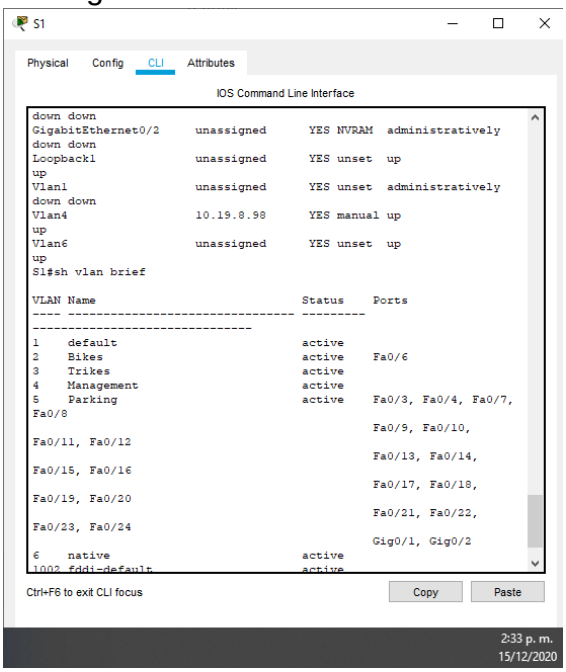
Tabla 5 Configurar en S2

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes S2(config)#vlan 2 S2(config-vlan)#name Bikes VLAN 3, name Trikes S2(config)#vlan 3 S2(config-vlan)#name Trikes VLAN 4, name Management S2(config)#vlan 4 S2(config-vlan)#name Management VLAN 5, nombre Parking S2(config)#vlan 5 S2(config-vlan)#name Parking VLAN 6, nombre Native S2(config)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6

Tarea	**Especificación**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación S2(config-if)#channel-group 1 mode active S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	permite 3 MAC addresses S2(config-if)#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 S2(config)#interface range fa0/5-17 , fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Interfaces sin uso S2(config-if-range)#sh

En la siguiente figura se puede evidenciar en el SW1 la configuración aplicada para habilitar las VLAN solicitadas en el ejercicio, igualmente vemos la configuración IP del la vlan 4 definida para administración.

Figura 6 Verificación VLANs S2



Fuente: Autor

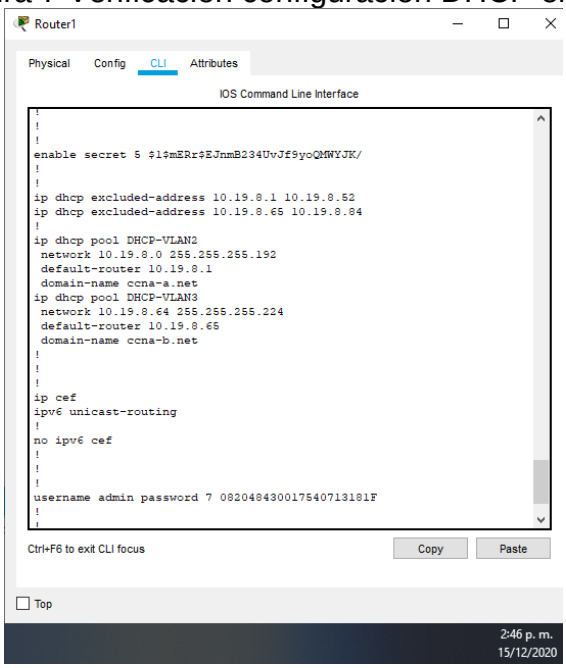
Continuando con el desarrollo del escenario 1 avanzamos ahora con la configuración en el Router 1 del enrutamiento por defecto el cual apuntara a la interfaz loopback configurada previamente, posteriormente configurare dos pools DHCP, uno para cada de las subinterfaces que se configuraron previamente sobre la interfaz GigaEthernet del mismo dispositivo, por último, se evidenciara que cada uno de los PC del proyecto recibirán la configuración IP por medio de este protocolo.

Tabla6. Configure R1

Tarea	**Especificación**
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada R1(config)#ip dhcp pool DHCP-VLAN2 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
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 R1(config)#ip dhcp pool DHCP-VLAN3 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

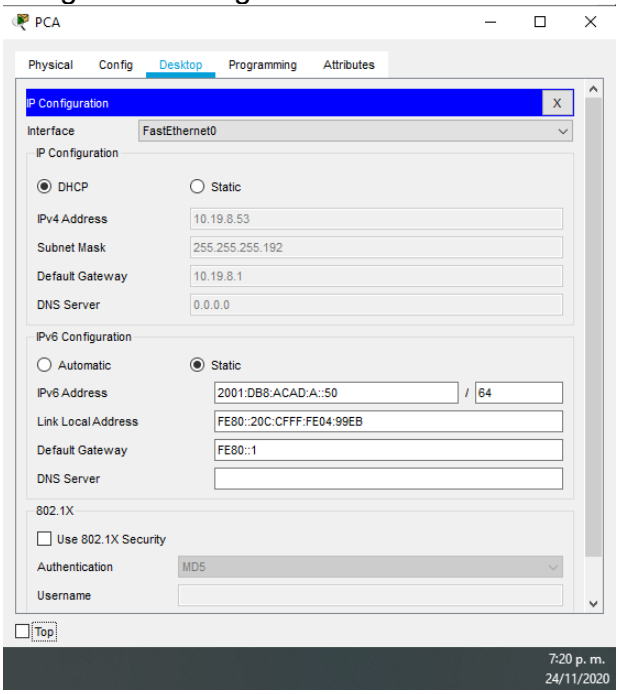
Ahora en la siguiente figura se puede evidenciar la configuración aplicada en el R1 para implementar el servicio de DHCP

Figura 7 Verificación configuración DHCP en R1



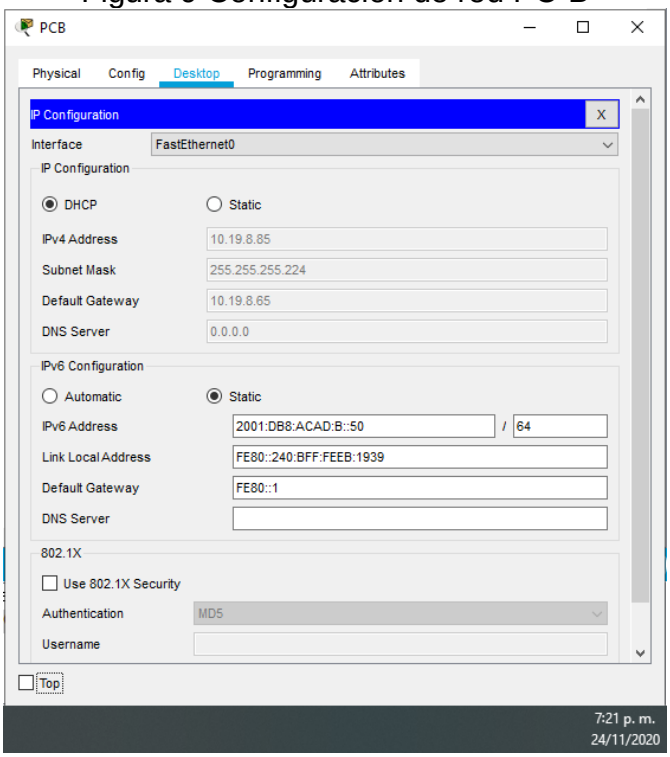
En las siguientes figuras se puede evidencias que los equipos adquieren correctamente direcciones IPV4 del servidor de DHCP

Figura 8 Configuración de red en PC-A



Fuente: Autor

Figura 9 Configuración de red PC-B



Fuente: Autor

Finalmente, luego de aplicar todas las configuraciones planteadas en el desarrollo de este escenario en la parte 3 se procede con las pruebas de conectividad por medio del comando PING entre los diferentes dispositivos.

Parte 3 Probar y verificar la conectividad de extremo a extremo:

A continuación, se evidencian las pruebas realizadas desde el PC-A hasta el R1, SW 1 y 2, igualmente hasta el PC y por ultimo las direcciones IPV4 e IPV6 de la interfaz loopback con la cual se está simulando una conexión a internet.

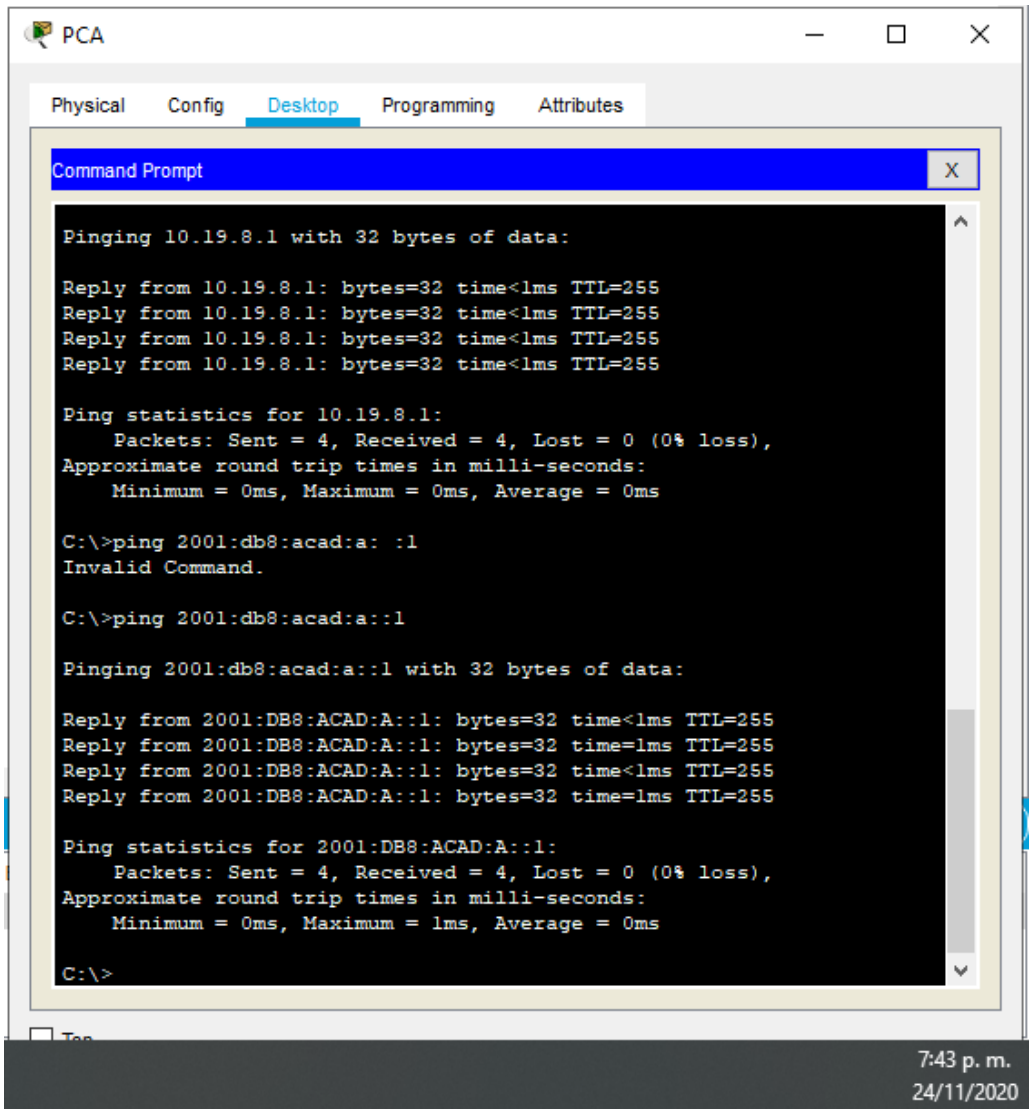
Se omiten algunos resultados con el fin de no hacer tan extenso este documento, sin embargo, como anexo se encuentra la simulación de este escenario en el cual es posible ejecutar las pruebas adicionales que se consideren.

Tabla 7. Prueba de PC-A hasta R1

Desde	A	de Internet	Dirección IP	Resultado
PC-A	R1, 0/0/1.2	Dirección	10.19.8.1	OK
		IPv6	2001:db8:acad:a::1	OK

Se realiza ping IPV4 e IPV6 desde el PC-A hasta el R1 subinterfaz 1.2 con resultado satisfactorio.

Figura 10 ping desde PCA hacia R1 G0/0/1.2



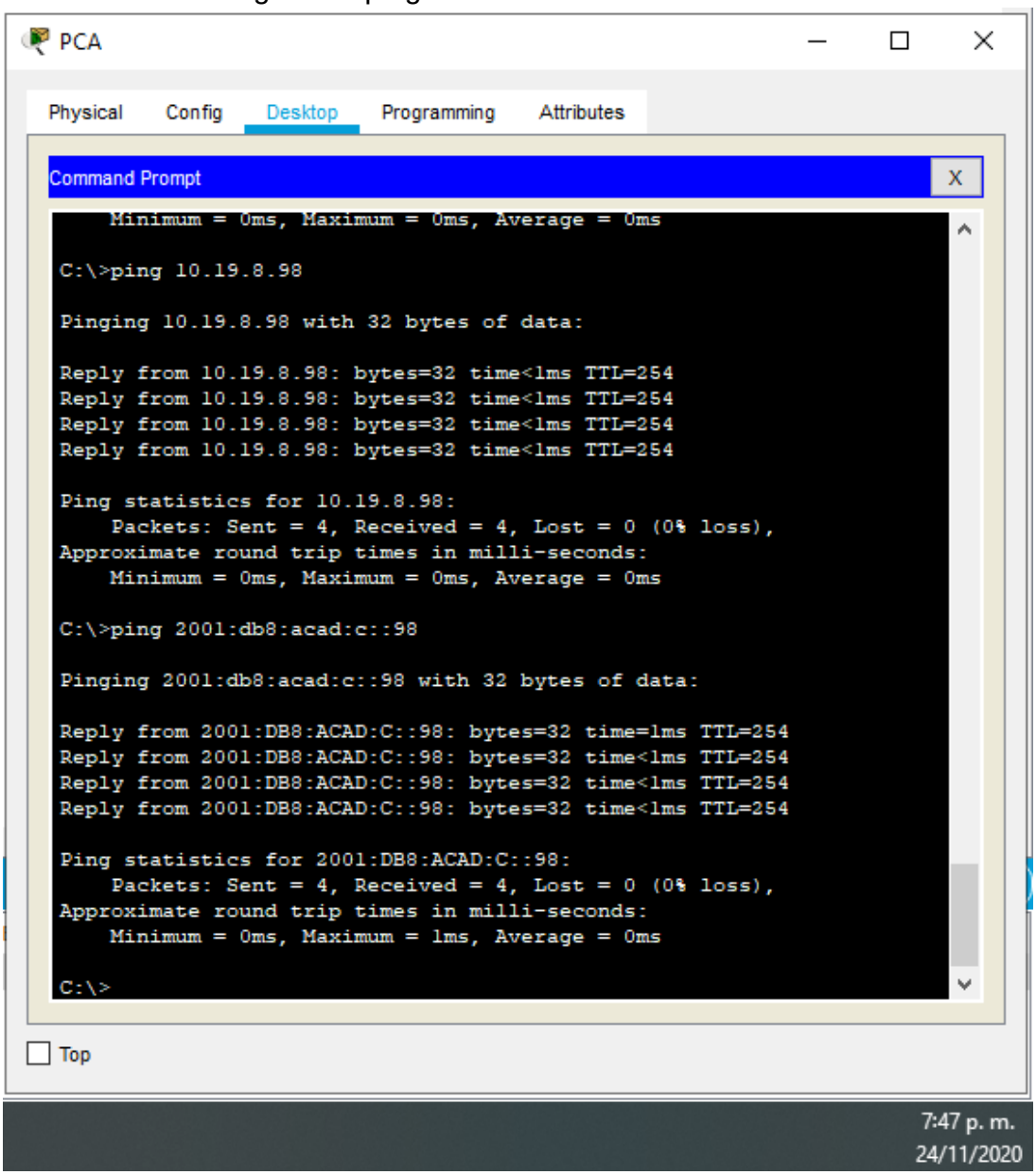
Fuente: Autor

Tabla 8. Prueba de PC-A hasta S1

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	S1,VLAN4	Dirección	10.19.8.98	OK
		IPv6	2001:db8:acad:c: :98	OK

Se realiza ping IPV4 e IPV6 desde el PC-A hasta el S1 con resultado satisfactorio.

Figura 11 ping desde PCA hacia S1 VLAN4



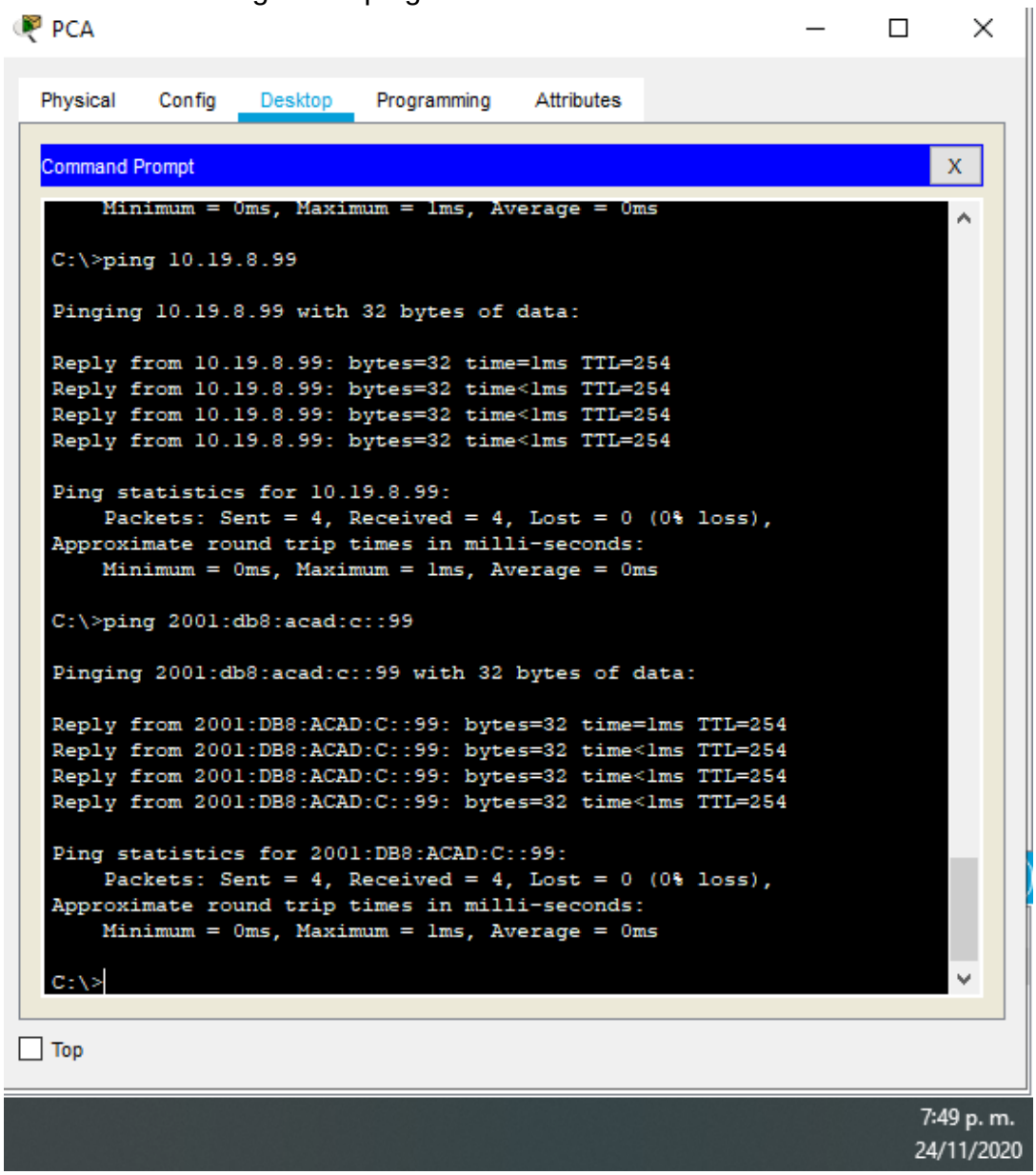
Fuente: Autor

Tabla 9. Prueba de PC-A hasta S2

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	S2,VLAN 4	Dirección	10.19.8.99.	OK
		IPV6	2001:db8:acad:c: :99	OK

Se realiza ping IPV4 e IPV6 desde el PC-A hasta el S2 con resultado satisfactorio.

Figura 12 ping desde PCA hacia S2 VLAN4



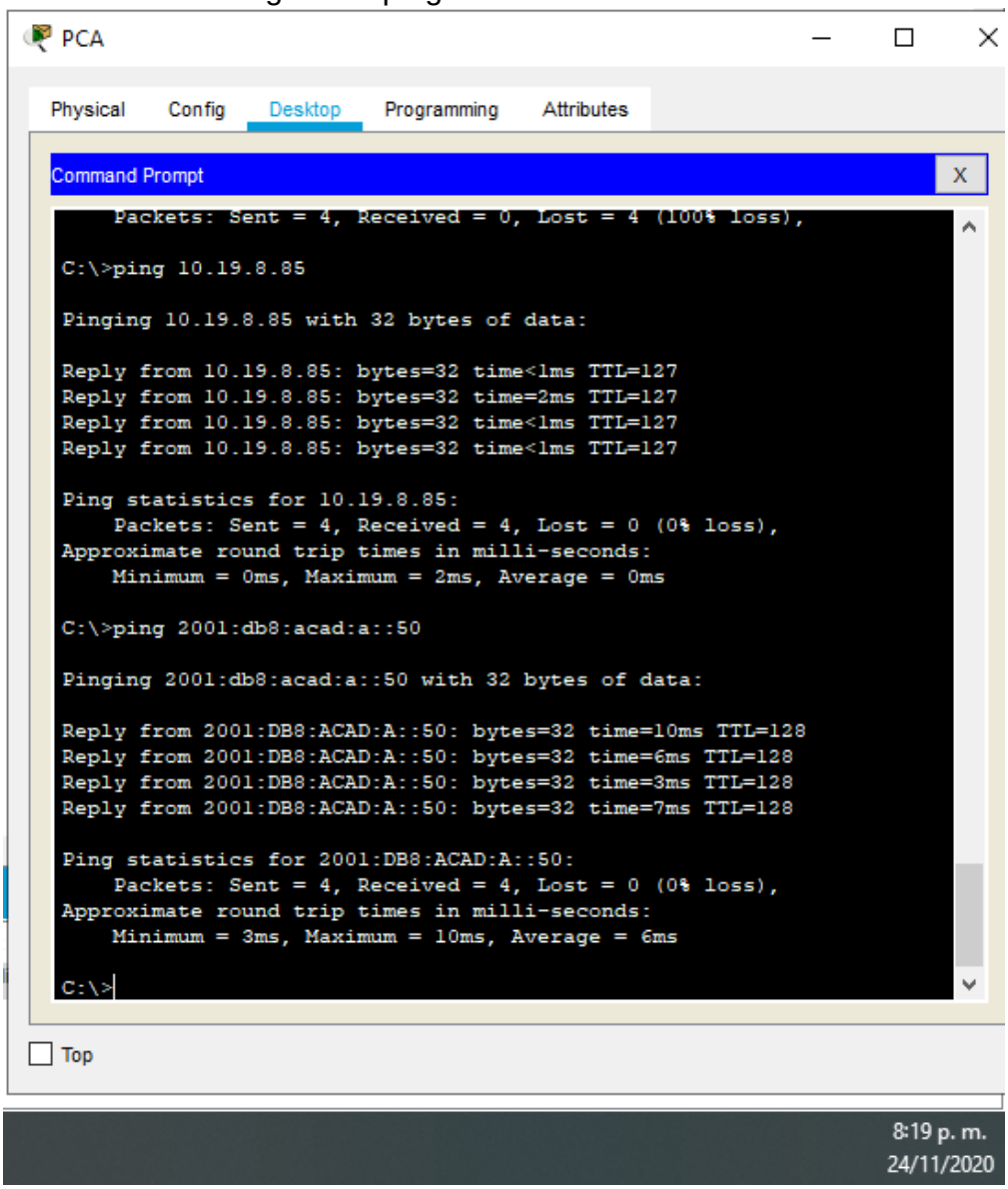
Fuente: Autor

Tabla 10. Prueba de PC-A hasta PC-B

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	PC-B	Dirección	10.19.8.85	OK
		IPV6	2001:db8:acad:b: :50	OK

Se realiza ping IPV4 e IPV6 desde el PC-A hasta el PC-B con resultado satisfactorio.

Figura 13 ping desde PCA hacia PCB

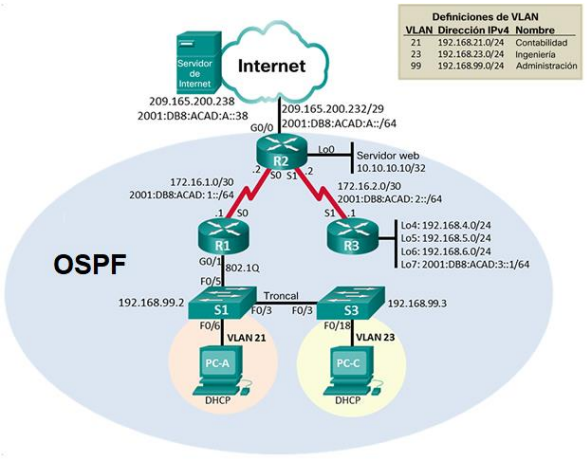


Fuente: Autor

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.

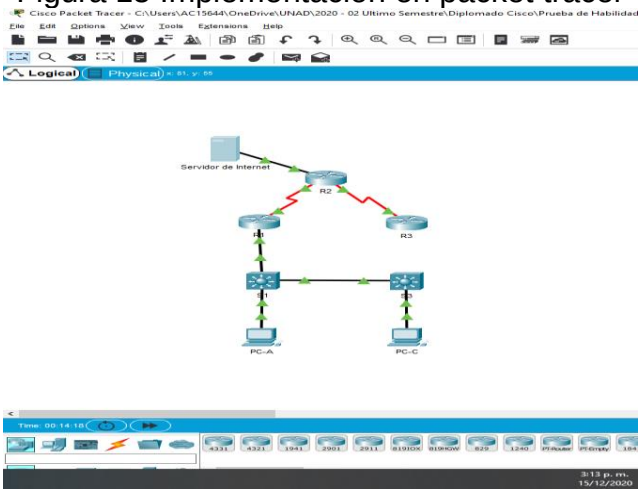
Figura 14 Topología escenario #2



Fuente: UNAD

A continuación, se presenta la figura 15 en la cual se puede evidenciar la implementación del escenario 2 en Packet tracer

Figura 15 Implementación en packet tracer



Fuente: Autor

Parte 1: Inicializar dispositivos

Inicializar y volver a cargar los routers y los switches

Como el desarrollo de esta prueba de habilidades se está desarrollando en Packet Tracer los dispositivos ya se encuentran en estado de fábrica.

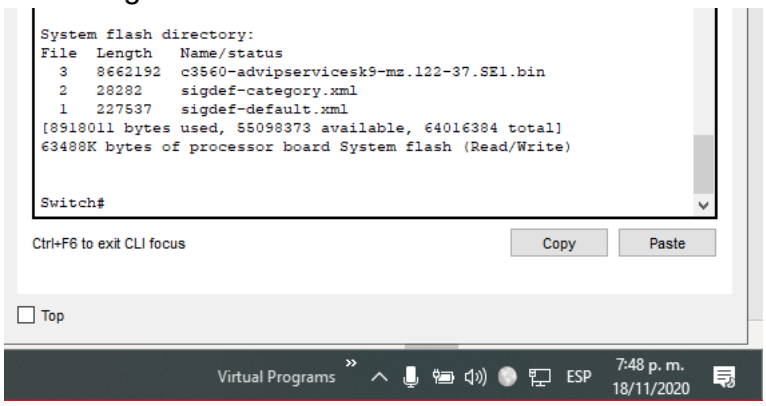
En esta parte inicial del escenario 2 realizaremos el borrado de tanto del archivo de configuración como de la base de datos en la que se almacenan las VLAN.

Tabla 11. Inicializar y volver a cargar los routers y los switches

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch#RELOAD
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash:

En la siguiente figura se evidencia que la base de datos de VLAN no esté en la memoria flash en ambos switches

Figura 16 verificación base de datos SW



Parte 2: Configurar los parámetros básicos de los dispositivos

En esta parte se realiza la configuración IP de un equipo servidor que estará simulando ser un servidor web ubicado en internet con direccionamiento público.

Tabla 12: Configurar la computadora de Internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	/28 255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

A continuación, en la tabla 14 se realizará la configuración inicial del R1, primero se desactiva la búsqueda de DNS, se reemplaza el nombre del dispositivo para poderlo identificar fácilmente y luego se configuran los parámetros de seguridad tanto para la conexión por consola como para el acceso remoto por medio de las líneas VTY, por último, establezco un mensaje de alerta que para todos aquellos que tengan intención de conectarse al dispositivo sean notificados con algún mensaje de interés.

También realizamos la configuración IPV4 e IPV6 sobre la interfaz Serial 0/0/0, por

último, en esta etapa configuraremos las rutas por defecto tanto en IPV4 como en IPV6.

Es importante mencionar que el procedimiento mencionado anteriormente se repite en las tablas 15 y 16 para los Router 2 y 3.

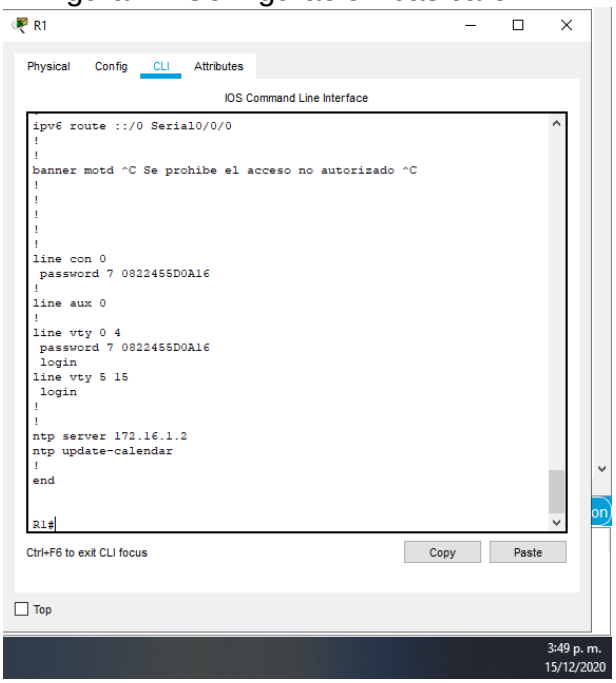
Tabla 13: Configurar R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco
Contraseña de acceso Telnet	Cisco R1(config)#line vty 0 4 R1(config-line)#pas R1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config-if)#description "CONEXION CON R2" R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh

Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 route ::/0 serial 0/0/0

En la siguiente figura se puede evidenciar la configuración básica inicial en el router 1, vemos que se aplica seguridad a las líneas VTY y consola.

Figura 17 Configuración básica en R1



Fuente: Autor

Tabla 14: Configurar R2

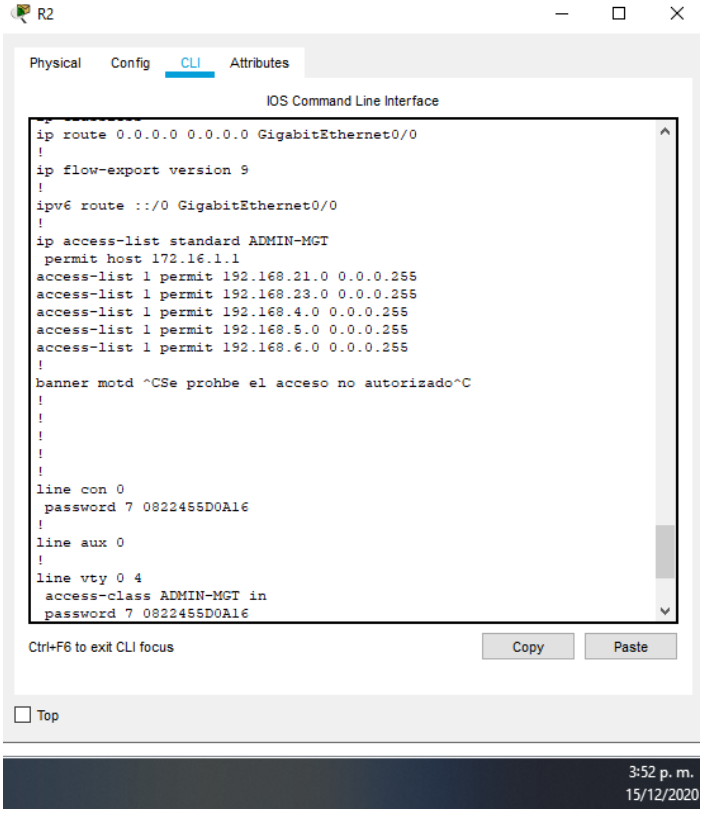
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class R2(config)#enable secret class

Contraseña de acceso a la consola	Cisco R2(config)#line console 0 R2(config-line)#password cisco
Contraseña de acceso Telnet	Cisco R2(config)#line vty 0 4 R2(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Habilitar el servidor HTTP	No es posible ejecutarlo desde Packet Tracer
Mensaje MOTD	Se prohíbe el acceso no autorizado. R2(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/0	Establezca la dirección IPv4. R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 Activar la interfaz R2(config-if)#no sh
Interfaz S0/0/1	Establecer la descripción R2(config-if)#description "CONEXION CON R3" Establezca la dirección IPv4. R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 201:db8:acad:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config-if)#description "CONEXION A INTERNET" Establezca la dirección IPv4. R2(config-if)#ip address 209.165.200.228 255.255.255.240 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz R2(config-if)#no sh

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)#description "CONEXION LOOPBACK" Establezca la dirección IPv4. R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ipv6 route ::/0 gigabitEthernet 0/0

En la siguiente figura se puede evidenciar la configuración básica inicial en el router 2, la configuración de las rutas por defecto IPV4 e IPV6 mas el aseguramiento de las líneas de consola y VTY.

Figura 18 Verificación rutas por defecto IPV4 e IPV6



Fuente: Autor

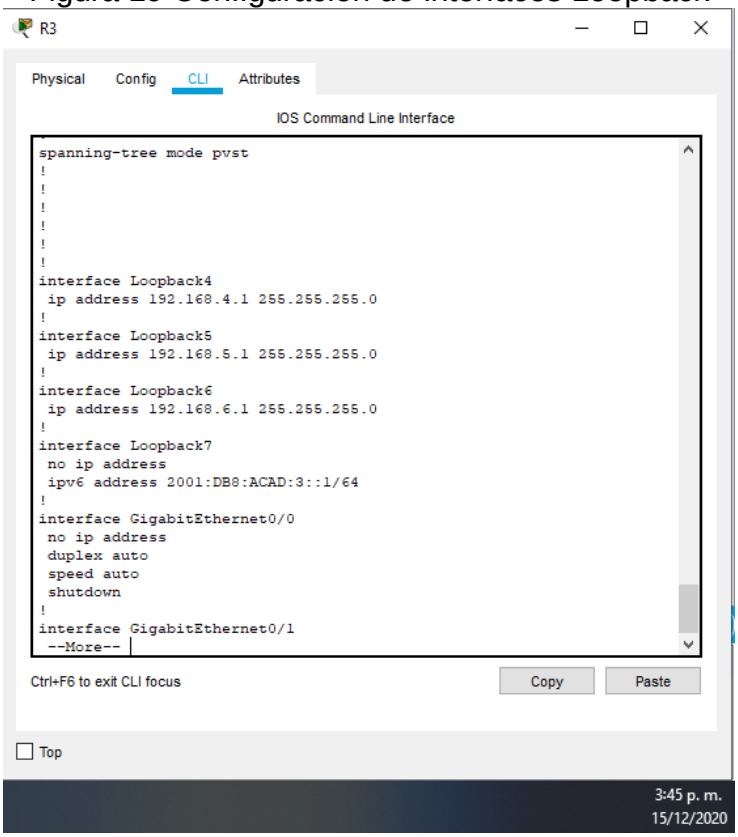
Tabla 15: Configurar R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	Cisco R3(config)#line console 0 R3(config-line)#password cisco
Contraseña de acceso Telnet	Cisco R3(config)#line vty 0 4 R3(config-line)#pas R3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)#banner motd "Se prohibe el acceso no autorizado"
Interfaz S0/0/1	Establecer la descripción: R3(config-if)#description "CONEXION CON R2" Establezca la dirección IPv4. R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 Activar la interfaz R3(config-if)#no sh
Interfaz loopback 4	Establezca la dirección IPv4. R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección IPv4. R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7	Establezca la dirección IPv6. R3(config-if)#ipv6 address 2001:db8:acad:3::1/64

En la siguiente figura podemos evidenciar la configuración realizada en el R3 de las interfaces Loopback

Figura 19 Configuración de interfaces Loopback



Fuente: Autor

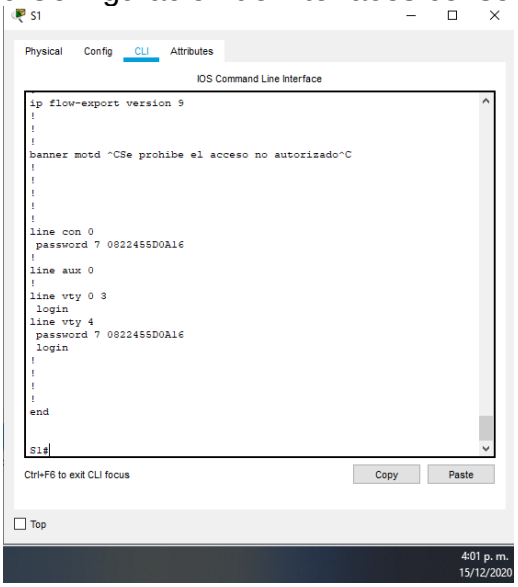
En esta etapa del proceso de simulación se realiza la configuración en los SW1 y 3, el proceso que se describe en las tablas 17 y 18 nos permitirá aplicar las configuraciones iniciales en los dos dispositivos, en los cuales se debe deshabilitar la búsqueda de DNS, posteriormente asignaremos los nombres correctos a los equipos, en la siguiente etapa se aseguran las conexiones entrantes tanto por consola como por las líneas VTY y adicionalmente es encriptan todas las contraseñas de los switch, finalmente se coloca un mensaje de alerta a los usuarios que intenten conectarse a los equipos.

Tabla 16: Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S1 Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Class S1(config)#enable secret class
Contraseña de acceso a la consola	Cisco S1(config)#line console 0 S1(config-line)#password cisco
Contraseña de acceso Telnet	Cisco S1(config)#line vty 04 S1(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S1(config)#banner motd "Se prohibe el acceso no autorizado"

En la siguiente figura se puede observar la configuración aplicada en SW 1 para definir un banner y la seguridad de las líneas de consola y VTY.

Figura 20 Configuración de interfaces consola y VTY



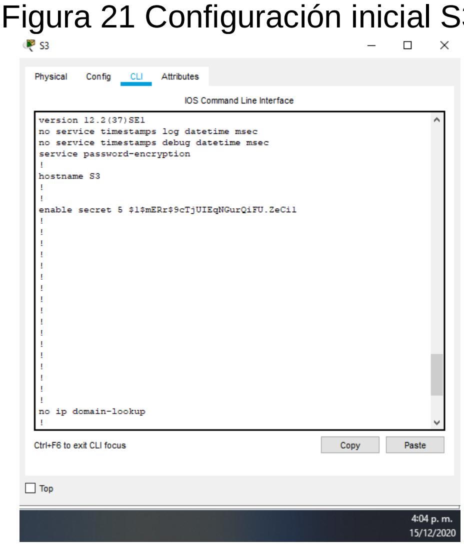
Fuente: Autor

Tabla 17: Configurar S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	S3 Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	Class S3(config)#enable secret class
Contraseña de acceso a la consola	Cisco S3(config)#line console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	Cisco S3(config)#line vty 0 4 S3(config-line)#password cisco
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S3(config)#banner motd "Se prohibe el acceso no autorizado"

En la siguiente figura se puede observar la configuración aplicada en SW 1 para definir el nuevo hostname, la contraseña de enable encriptada y la desactivación de la búsqueda de dominios.

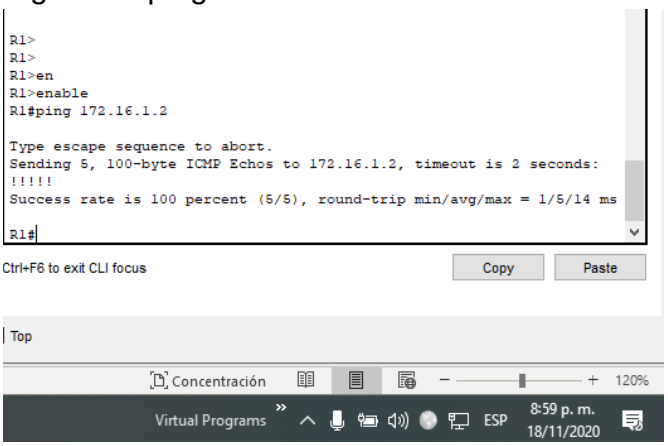
Figura 21 Configuración inicial S3

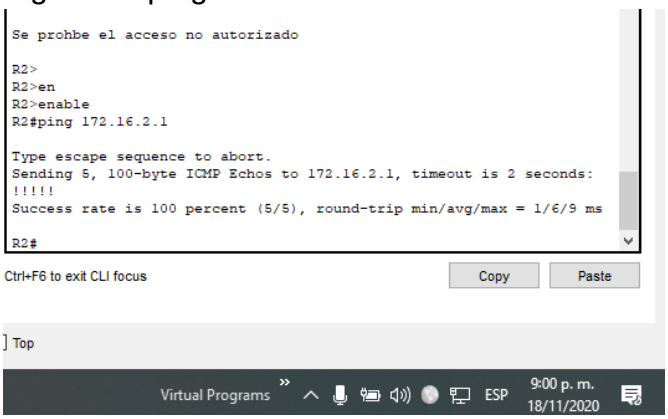
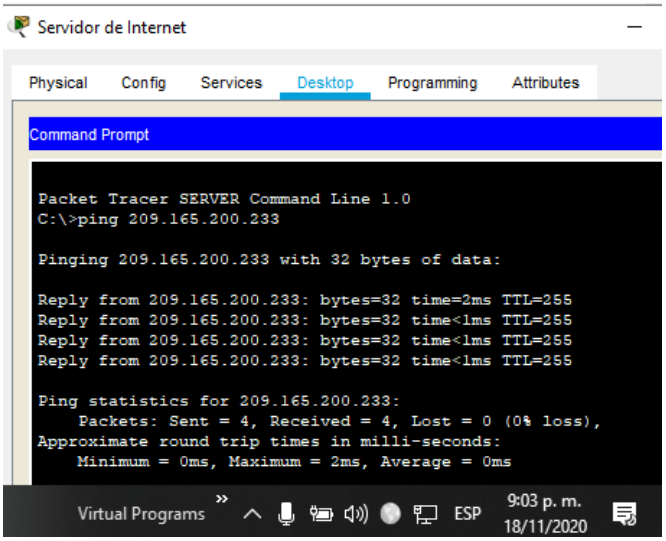


Fuente: Autor

Luego de aplicar las configuraciones previas donde se aseguraron los dispositivos y se adicionaron las configuraciones IP podemos proceder con las pruebas de conectividad entre los dispositivos R1 y R2, R2 y R3 y desde el PC hasta su default gateway.

Tabla 18: Verificar la conectividad de la red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	En la siguiente figura podemos apreciar el resultado del ping entre el Router 1 y el Router 2, este es correcto: Figura 22 ping desde R1 hacia R2  Fuente: Autor

R2	R3, S0/0/1	172.16.2.1	En la siguiente figura podemos apreciar el resultado del ping entre el Router 2 y el Router 3, este es correcto: Figura 23 ping desde R2 hacia R3  Fuente: Autor
PC de Internet	Gateway predeterminado	209.165.200.233	En la siguiente figura podemos apreciar el resultado del ping entre el PC de Internet y el Gateway Predeterminado, este es correcto: Figura 24 ping desde PC Internet hacia Gateway Predeterminado  Fuente: Autor

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

Luego de comprobar que la conectividad entre los dispositivos es correcta procedemos con el proceso de configuración de las VLAN en los switch,

lo cual incluye crear las VLAN, configurar puertos en modo acceso y troncales además también se asignarán las VLAN que corresponde a cada puerto y por último apagaremos los puertos no utilizados.

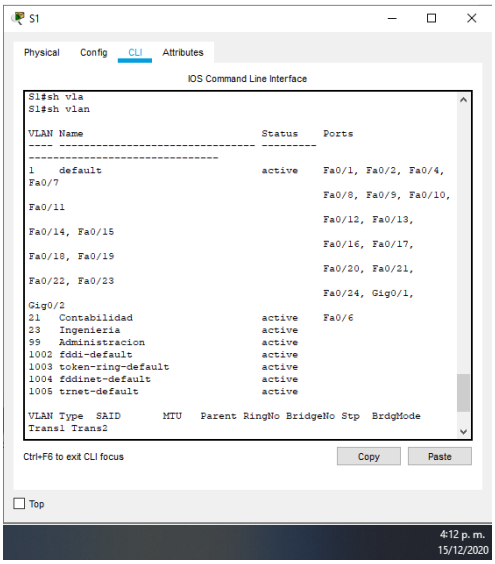
Tabla 19: Configurar S1

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 S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. S1(config-if)#interface vlan 99
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface fastEthernet 0/3 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#interface range fastEthernet 0/1 - 2 S1(config-if-range)#switchport mode access S1(config)#interface fastEthernet 0/4 S1(config-if-range)#switchport mode access S1(config)#interface range fastEthernet 0/6 - 24 S1(config-if-range)#switchport mode access S1(config)#interface range gigabitEthernet 0/1 - 2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range fa0/7 -24 S1(config-if-range)#sh S1(config)#interface range fastEthernet 0/1 -2 S1(config-if-range)#sh S1(config)#interface fastEthernet 0/4 S1(config-if)#sh S1(config)#interface range gigabitEthernet 0/1 - 2 S1(config-if-range)#sh

En la siguiente figura se puede evidenciar en el SW1 la configuración aplicada para habilitar las VLAN solicitadas en el ejercicio

Figura 25 Configuración VLAN S1



Fuente: Autor

Tabla 20: Configurar S3

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. S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config)#vlan 99 S3(config-vlan)#name Administracion
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#inter fa0/3 S3(config-if)#switchport trunk encapsulation dot1q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range fa0/1 - 2 S3(config-if-range)#switchport mode access S3(config)#interface range fa0/4 - 17 S3(config-if-range)#sw mo access S3(config)#interface range fa0/19 - 24 S3(config-if-range)#switchport mode access S3(config)#interface range gigabitEthernet 0/1-2 S3(config-if-range)#switchport mode access

Asignar F0/18 a la VLAN 23	S3(config)#inter fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#interface range fa0/1 - 2 S3(config-if-range)#sh S3(config-if-range)#interface range fa0/4 - 17 S3(config-if-range)#sh S3(config-if-range)#interface range fa0/19 - 24 S3(config-if-range)#sh S3(config-if-range)#interface range gigabitEthernet 0/1-2 S3(config-if-range)#sh

Luego configurar previamente en los SW las VLAN, los puertos troncales, y la seguridad, avanzaremos con la configuración del encapsulamiento dot1Q y las subinterfaces en el Router 1

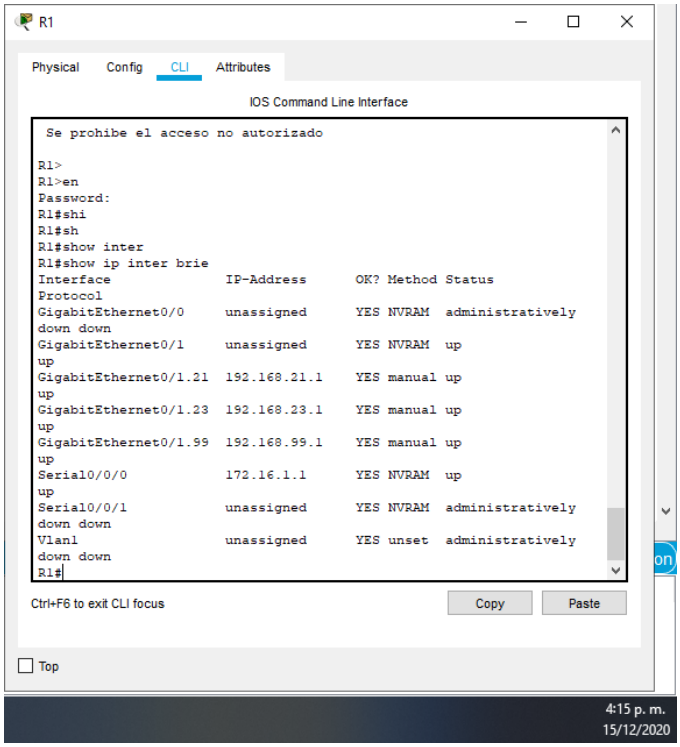
Tabla 21: Configurar R1

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 R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description "CONTABILIDAD" R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#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 R1(config)#interface g0/1.23 R1(config-subif)#description "INGENIERIA" R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#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 R1(config)#interface g0/1.99 R1(config-subif)#description "ADMINISTRACION" R1(config-subif)#ENcapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#no sh

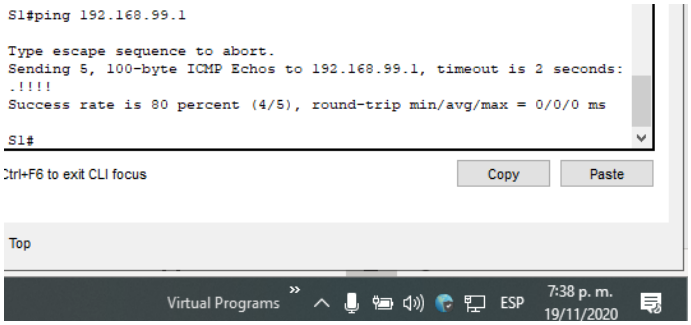
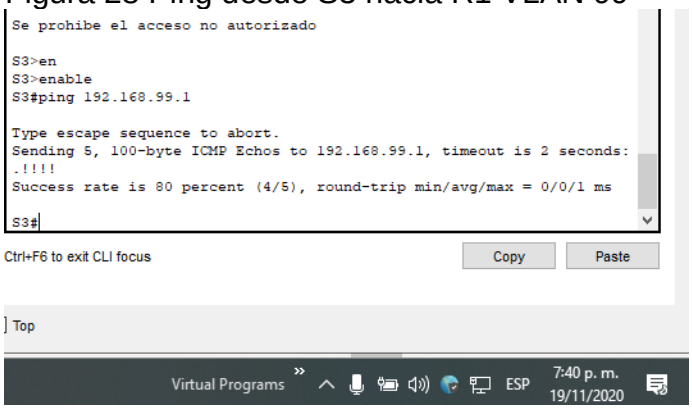
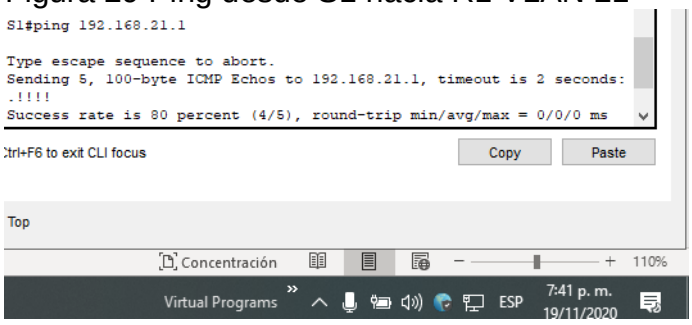
Ahora podemos evidenciar la configuración que fue aplicada en el R1 para habilitar las subinterfaces y el encapsulamiento.

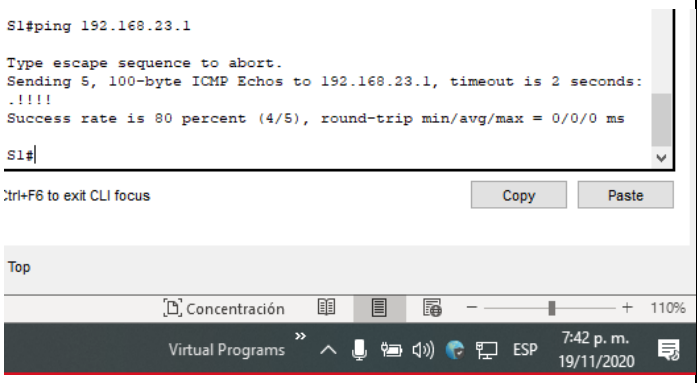
Figura 26 Configuracion R1 Subinterfaces



Ahora que témenos configuradas las VLAN en los SW definidos también los puertos troncales y el encapsulamiento y las subinterfaces en el Router 1 podemos proceder con las pruebas de conectividad desde cada una de las VLAN hasta el Router 1.

Tabla 22: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Prueba de ping desde el S1 hasta el R1 Figura 27. Ping desde S1 hacia R1 VLAN 99  Fuente: Autor
S3	R1, dirección VLAN 99	192.168.99.1	Prueba de ping desde el S3 hasta el R1 Figura 28 Ping desde S3 hacia R1 VLAN 99  Fuente: Autor
S1	R1, dirección VLAN 21	192.168.21.1	Prueba de ping desde el S1 hasta el R1 Figura 29 Ping desde S1 hacia R1 VLAN 21  Fuente: Autor

S3	R1, dirección VLAN 23	192.168.23.1	Prueba de ping desde el S3 hasta el R1 Figura 30 Ping desde S3 hacia R1 VLAN 23  Fuente: Autor

Como el resultado de las pruebas anteriores fue satisfactorio podemos avanzar a continuación con la configuración de nuestro protocolo de enrutamiento, para este caso práctico se elegio OSPF, es por esto que veremos en las tablas 24, 25 y 26 como habilitar este protocolo en los routers, también se anunciaran las redes que conoce cada uno de ellos y por ultimo definiremos cuales son las interfaces pasivas, es decir por qué interfaz o interfaces no queremos enviar anuncios o/y actualizaciones OSPF.

Parte 4: Configurar el protocolo de routing dinámico OSPF

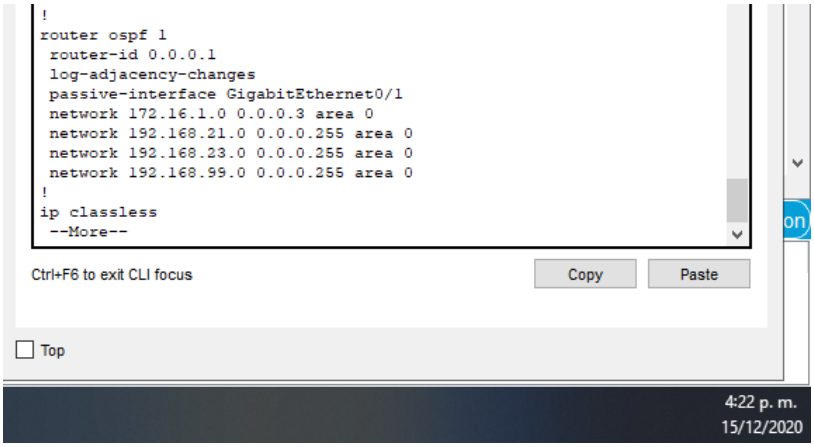
Tabla 23: Configurar OSPF en el R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 0.0.0.1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0

Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1

A continuación, en la figura podemos visualizar las configuraciones aplicadas en el R1 para habilitar el protocolo de enrutamiento OSPF.

Figura 31 Verificación de configuración OSPF R1



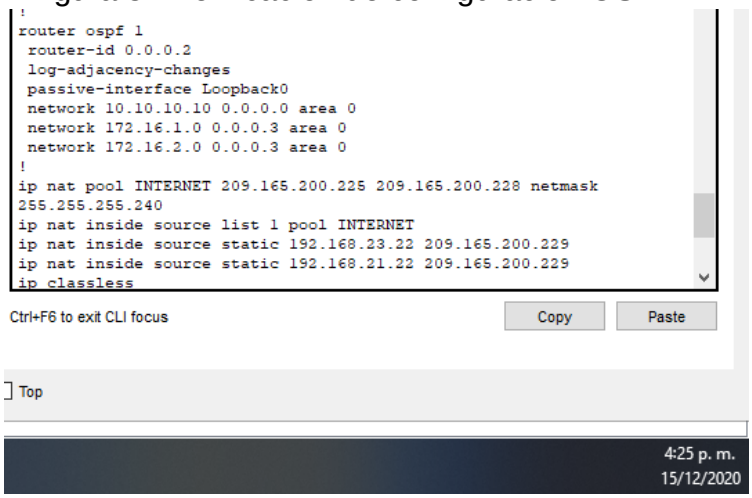
Fuente: Autor

Tabla 24: Configurar OSPF en el R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 0.0.0.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface lo0

A continuación, en la figura podemos visualizar las configuraciones aplicadas en el R2 para habilitar el protocolo de enrutamiento OSPF.

Figura 32 Verificación de configuración OSPF R2



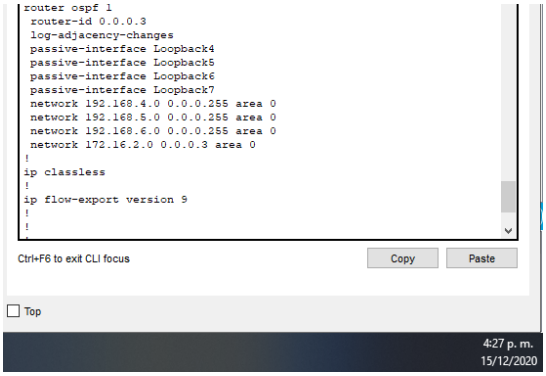
Fuente: Autor

Tabla 25: Configurar OSPF en el R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 0.0.0.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0 R3(config-router)#network 172.16.2.0. 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#passive-interface lo7

A continuación, en la figura podemos visualizar las configuraciones aplicadas en el R2 para habilitar el protocolo de enrutamiento OSPF.

Figura 33 Verificación de configuración OSPF R3



Fuente: Autor

A continuación, se muestran los comandos con los cuales se pueden hacer las verificaciones luego de la implementación del protocolo de enrutamiento OSPF sobre la implementación

Tabla 26: Verificar la información de OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip ospf 1 interface
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf 1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip ospf neighbor

Parte 5: Implementar DHCP y NAT para IPV4

Ahora en la parte 5 de este escenario se trabajará una parte importante de este desarrollo, el servicio DHCP es una de las herramientas vitales para cualquier administrador de grandes redes, pues por medio de él se pueden hacer implementaciones y despliegues masivos de dispositivos finales ya que este se encarga de responder las peticiones de los equipos que no tienen una dirección IP y que poseen el servicio de DHCP cliente.

Por otra parte, también se configurará el servicio de NAT el cual se puede implementar de forma estática o dinámica, con el NAT podemos permitir que

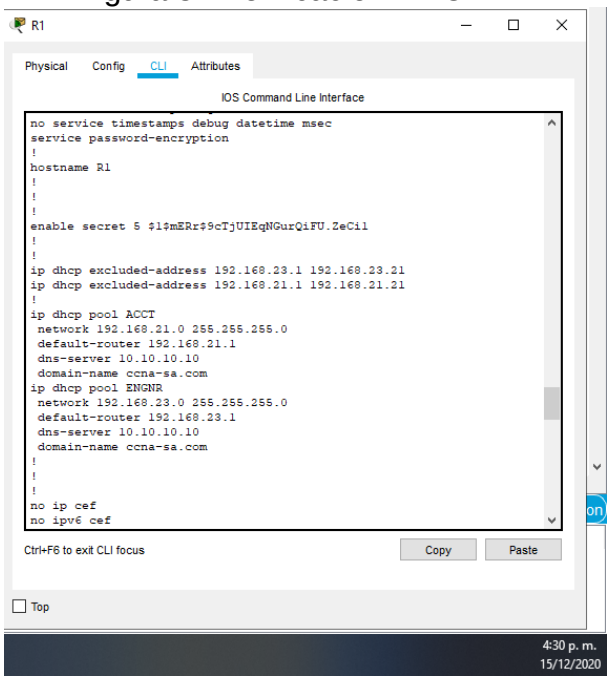
muchos dispositivos de la red interna puedan salir a navegar en el mundo de internet con una sola o varias direcciones IPV4 públicas, esto claramente no se aplica para IPV6 debido al número casi infinito de direcciones que posee esa versión.

Tabla 27: Configurar el R1 como 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	192.168.21.1 – 192.168.21.21 R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.21
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	192.168.23.1 – 192.168.23.21 R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.21
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 R1(config)#ip dhcp pool ACCT 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)#network 192.168.21.0 255.255.255.0
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 R1(config)#ip dhcp pool ENGNR 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)#network 192.168.23.0 255.255.255.0

Ahora en la siguiente figura se puede evidenciar la configuración aplicada en el R1 para implementar el servicio de DHCP

Figura 34 Verificación DHCP R1



Fuente: Autor

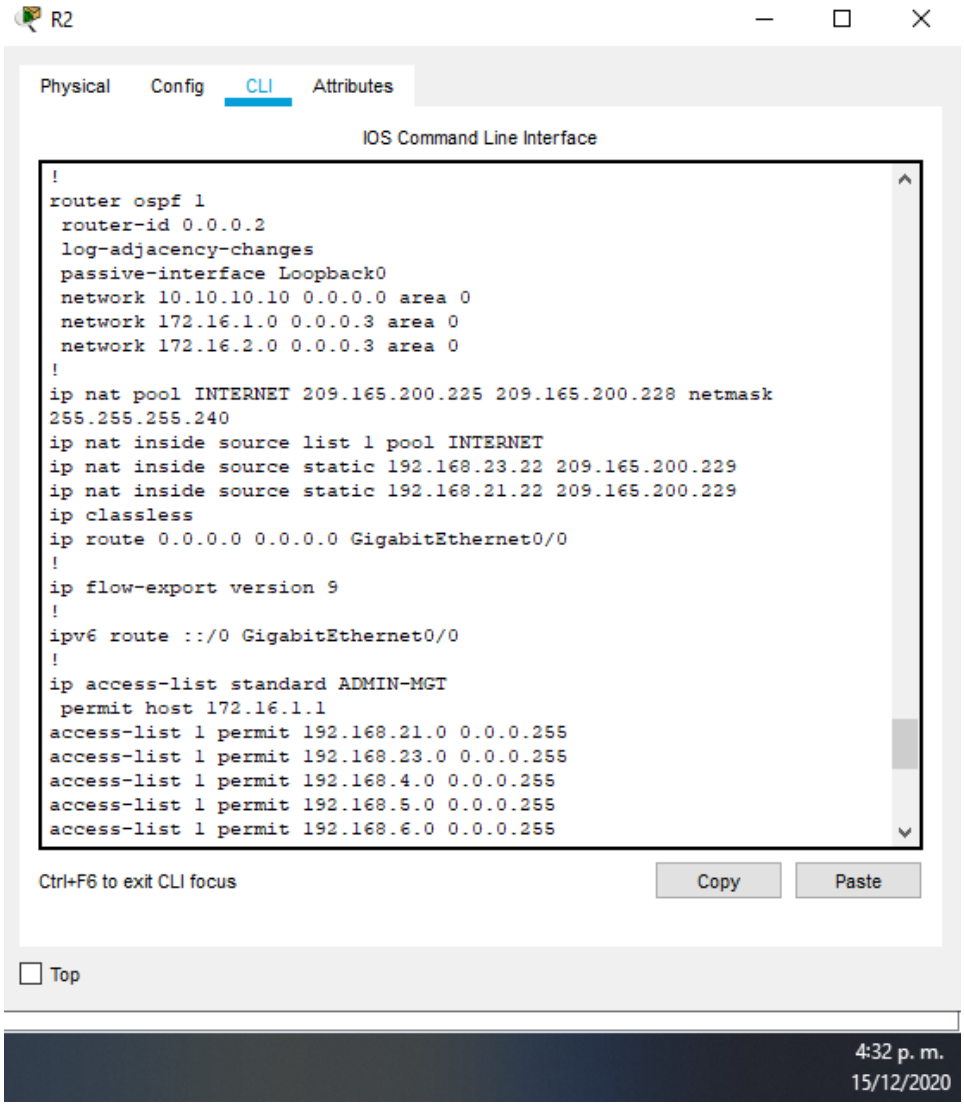
Tabla 28: Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 password cisco12345

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)#ip nat inside source static 192.168.21.22 209.165.200.229 R2(config)#ip nat inside source static 192.168.23.22 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0 R2(config-if)#ip nat outside R2(config)#inter ser 0/0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#ip nat inside source list 1 pool INTERNET Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
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** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.240

En la siguiente figura se puede apreciar la configuracion aplicada al R2 para habilitar el NAT estático y dinámico:

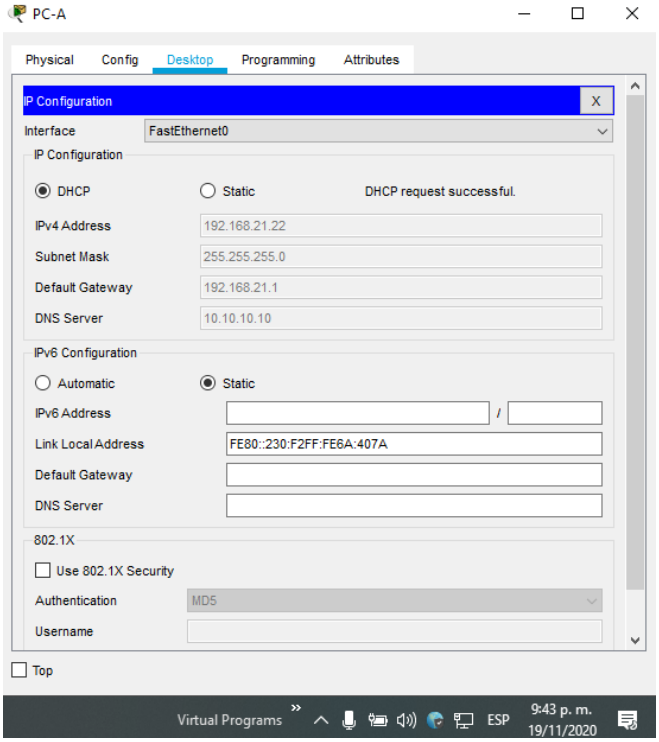
Figura 35 Verificacion NAT estático y dinámico

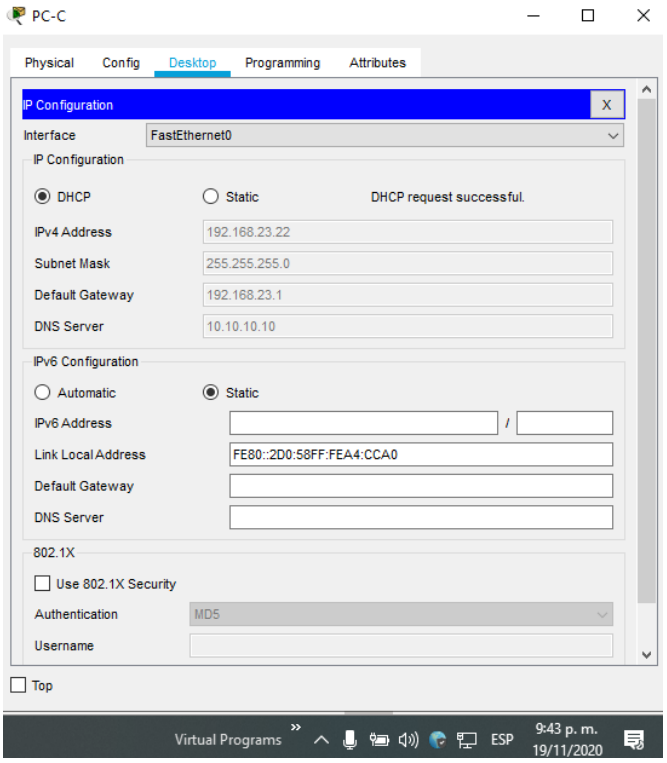


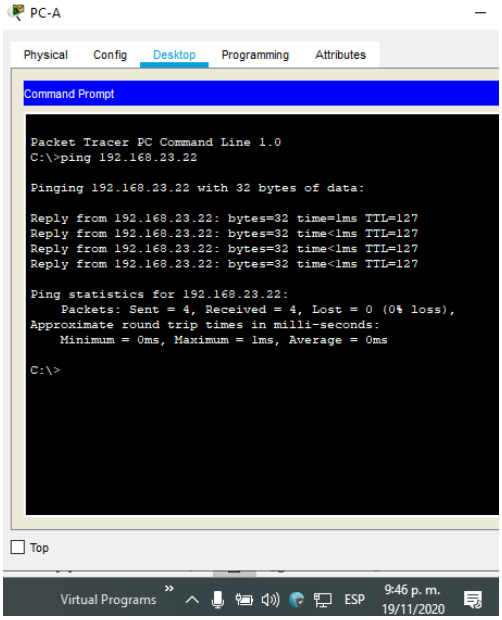
Fuente: Autor

Ahora que hemos configurado el servicio de DHCP y el NAT podemos verificar desde cada uno de los PC que este recibiendo los parámetros IP que corresponden a la VLAN que pertenece:

Tabla 29: Verificar el protocolo DHCP

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	En la siguiente Figura se evidencia que el PC-A Adquiere correctamente direccionamiento desde el servidor DHCP Figura 36 Verificar que PC-A Adquiere dirección IP Por DHCP  Fuente: Autor

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	En la siguiente Figura se evidencia que el PC-C Adquiere correctamente direccionamiento desde el servidor DHCP Figura 37 Verificar que PC-C Adquiere dirección IP Por DHCP  Fuente: Autor

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	En la siguiente figura re evidencia que el PC-A puede hacer Ping de forma correcta al PC-C Figura 38 Ping desde PC-A hacia PC-C  Fuente: Autor

De acuerdo con las imágenes anteriores se evidencia que el desarrollo de las configuraciones fue correcto por lo cual ambos equipos recibieron dirección IP e igualmente el ping entre ambos responde con tiempos menores a 1ms.

Parte 6: Configurar NTP

Parte de una buena administración de una red y un elemento que es fundamental para temas de auditoria, diagnósticos y evaluaciones post mortem es tener una perfecta sincronía en la hora y fecha de los dispositivos de la red, es por esto por lo que a continuación se realizara la configuración del servicio NTP, en este se definirá que el R2 sea el servidor NTP y R1 se comportara como un cliente.

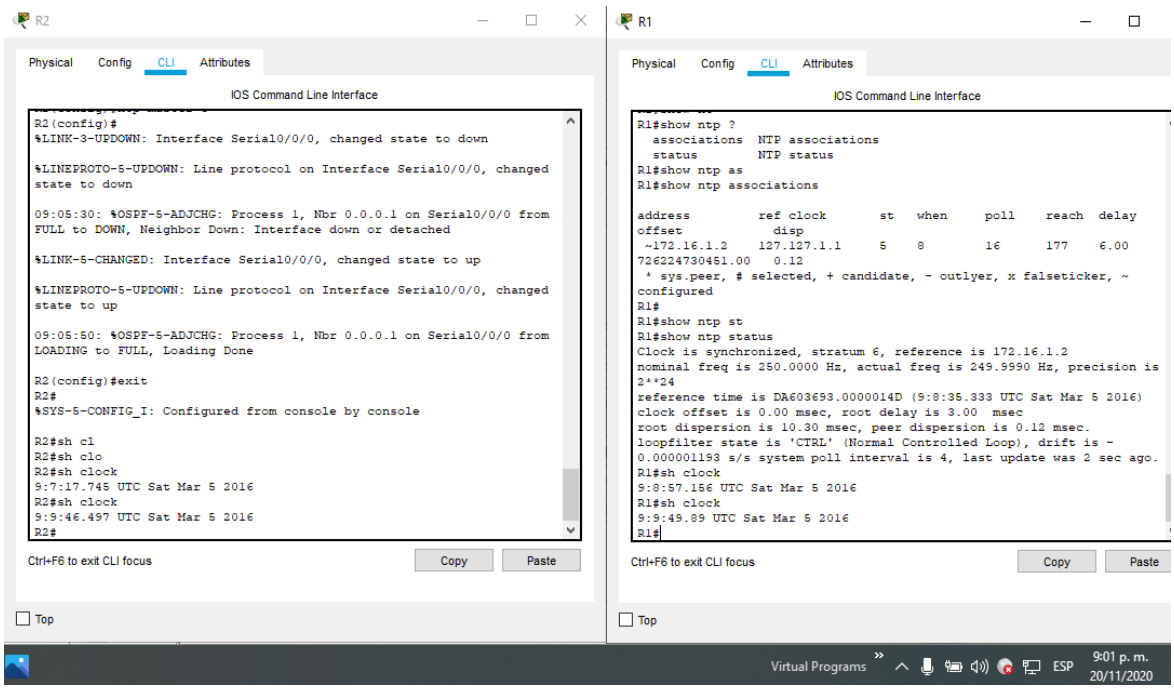
Tabla 30: Establecer la configuración NTP Cliente – Servidor

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:00:00 mar 5 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1:

En las siguientes figuras se puede evidenciar como el R1 sincroniza correctamente el reloj y la fecha desde el servidor NTP que fue configurado en R2

Figura 39 Verificación Servicio NTP Cliente – Servidor



Fuente: Autor

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

En esta última parte del trabajo se abordará el tema de las ACL o listas de control de acceso, con esto es posible aplicar políticas a los Router con el fin de permitir o denegar acceso a ciertos servicios, también es posible permitir o denegar conexiones vía telnet como lo veremos en el ejemplo realizado a continuación.

Tabla 31: 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** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in

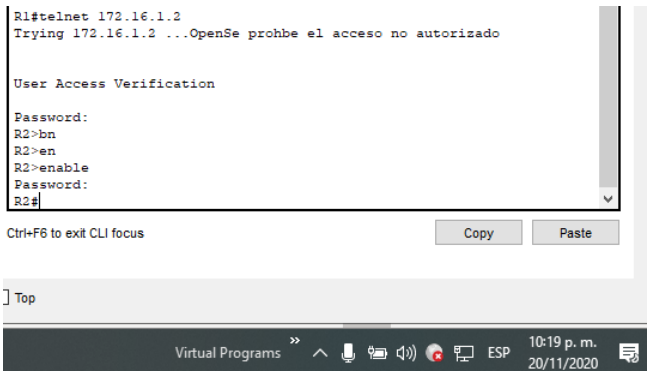
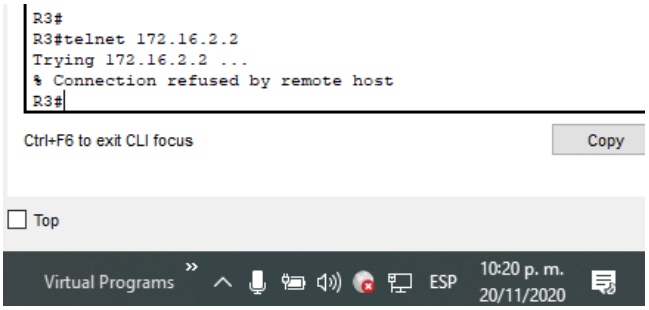
Verificar que la ACL funcione como se espera	En la verificación de la política se evidencia que el R1 puede acceder vía telnet. Figura 40 Desde R1 se tiene acceso vía Telnet:  Fuente: Autor En la verificación de la política se evidencia que el R3 no se puede acceder vía telnet. Figura 41 Desde R3 no se tiene acceso vía Telnet  Fuente: Autor En la verificación de la política se evidencia que los paquetes están haciendo match con la política implementada.

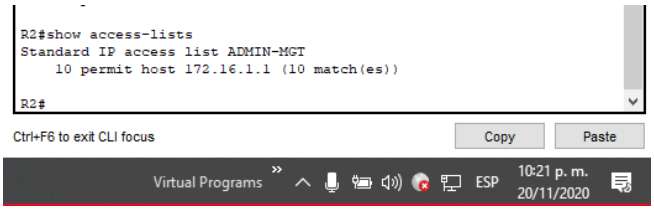
	Figura 42 La política hace match  Fuente: Autor

Tabla 32: 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	R2#show access-lists Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (10 match(es))
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ADMIN-MGT R2#show access-lists Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.228 172.16.1.2 --- ---
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

CONCLUSIONES

Con el desarrollo de esta actividad de simulación se logró poner a prueba todos los conocimientos adquiridos durante el programa académico con la simulación de los escenarios propuestos.

En el escenario uno se trabajó prácticas que permitieron medir la destreza para implementar redes LAN segmentadas por VLAN, estas se aplicaron la configuración por cada puerto dependiendo de la funcionalidad seleccionada (Access, Trunk) igualmente se implementó entre los Switch Cisco el servicio de EtherChannel el cual nos permitió evidencia como se pueden definir mecanismos de seguridad en caso de fallas físicas de un puerto, así mismo se evidencio por medio de la practica la implementación de una red sobre IPV6 y las diferencias principales respecto a su antecesora IPV4

Por su parte en el escenario 2 la practica recibió un enfoque más dirigido a la implementación de una red WAN en la cual se utilizó como protocolo de enrutamiento OSPF y sus características, se simulo una conexión a internet la cual debía hacer traslación de dirección privadas a publicas utilizando tanto NAT estática como dinámica, igualmente en esta parte se retomaron los conceptos LAN vistos en el escenario anterior como fueron DHCP, VLAN e IPV6, al mismo tiempo se implementó el servicio de NTP el cual permitió que los Router clientes pudieran establecer su configuración de hora y fecha tomándola del equipo que fue definido para esto.

BIBLIOGRAFIA

ACL (2019): ACL: Lista de Control de Accesos Recuperado de

https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

DHCP (2018): Qué es DHCP y cómo funciona. Recuperado de https://www.networkworld.es/telecomunicaciones/que-es-dhcp-y-como-funciona

NAT: Conversión de direcciones de red (NAT) Recuperado de

https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_71/rzajb/rzajbrzajb4natsd.htm

OSPF: OSPF (Open Shortest Path First) Recuperado de

https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_71/rzajw/rzajwospf.htm

VLAN (2020): Qué es una VLAN Recuperado https://ccnadesdecero.com/curso/vlan/

ANEXOS:

- Enlace a la carpera con los escenarios de simulación en Packet Tracer
- Enlace a la carpeta donde este contenido el articulo científico

  https://1drv.ms/u/s!AmrYqpfX4-8agbdPK41ag_6YOEYuNA?e=ieGgfB

IMPLEMENTACIO DE UN ESCENARIO PRACTICO UTILIZANDO LA HERRAMIENTA PACKET TRACER CON USO DE TECNOLOGÍA CISCO

Wilfer Velez Orozco
Universidad Nacional Abierta y a Distancia UNAD, velezo@unadvirtual.edu.co

Resumen

Por medio de la modalidad de "Proyecto Aplicado" el cual es desarrollado sobre un ambiente de simulación en Packet Tracer, herramienta de propiedad del gigantesco fabricante de dispositivos comunicaciones CISCO y que permite a los estudiantes de telecomunicaciones simular entornos prácticamente similares a los que se enfrentarían con equipos físicos reales.

Inicialmente se definen los elementos con los cuales se realizará la práctica, en este punto se deberán elegir los mas adecuados y que se ajusten según los requerimientos del ejercicio planteado.

La temática elegida en el curso CNNA que se abordaran durante el desarrollo del escenario son los siguientes: análisis inicial del diagrama propuesto, análisis de las tablas de direccionamiento y tabla de VLANs, posteriormente se configuraran los parámetros básicos en los dispositivos como la seguridad, los nombres así mismo los parámetros IP en las interfaces, en la siguiente etapa se implementaran las VLAN, se asignaran los puertos de acceso y troncales por último el EtherChannel.

En la fase final se habilitará desde el Router el protocolo DHCP y se deberá probará conectividad entre todos los dispositivos.

Palabras claves: **CISCO, LAN, WAN, VLAN, DHCP, EherChannel**

***Abstract*:**
Through the Applied project modality which is developed on a simulation environment in Packet Tracer, a tool owned by the giant manufacturer of communications devices CISCO and that allows telecommunications students to simulate environments practically similar to those they would face with equipment real physicists.

Initially the elements with which the practice will be carried out are defined, at this point the most appropriate ones must be chosen and adjusted according to the requirements of the proposed exercise.

The topics chosen in the CNNA course that will be addressed during the development of the scenario are the following: initial analysis of the proposed diagram, analysis of the addressing tables and VLANs table, later the basic parameters will be configured in the devices such as security, Also names the IP parameters in the interfaces, in the next stage the VLANs will be implemented, the access ports and trunks will be assigned finally the EtherChannel.

In the final phase, the DHCP protocol will be enabled from the Router and connectivity between all devices must be tested.

Keywords: **CISCO, LAN, WAN, VLAN, DHCP EtherChannel**

I. INTRODUCCION

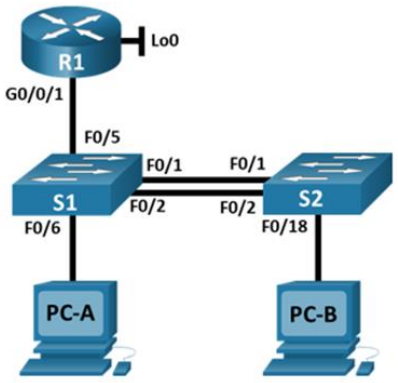
En la actualidad las comunicaciones se han convertido en parte fundamental de la operación en de casi cada dispositivo electrónico, el internet de las cosas llego para quedarse tanto en los ambientes familiares como empresariales por esta razón cada vez es común ver como la demanda de personas expertas en la implementación de redes de comunicaciones que integren deferentes aspectos como la escalabilidad, la seguridad la convergencia y a su vez que los diseños sean lo mas optimizados posibles para tener costos razonables.

METODOLOGIA

Se plantea un escenario en la figura 1 en el cual con la estructura de la red y las tablas de direccionamiento y VLANs se deberá implementar sobre la herramienta Packet Tracer el esquema que se mencionó anteriormente

El resultado final será garantizar el correcto funcionamiento de la red, la conectividad entre los dispositivos y la asignación de direccionamiento IP para cada una de las VLAN desde el router via DHCP

Topología de red escenario 1



Lista de direccionamiento IP

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

Lista de Vlans

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

Se da inicio con la inicialización de los dispositivos, estos comprenden el borrado de la configuración almacenadas en la memoria interna y las tablas de VLAN, se activa la configuración de la plantilla SDM para la admisión de IPv6.

Posteriormente se realiza la implementación de los elementos básicos como son la seguridad de los dispositivos, los accesos remotos permitidos, la configuración IPV4 e IPV6 de las interfaces y las rutas por defecto, los comandos ejecutados se presentan en las Tablas 1 y 2

Tabla 1
Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Escenario 1 Ivan Caro R1"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

A continuación en la tabla 2 realizamos la configuración inicial de los SW

Tabla 2 Configurar los Switch S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup Switch0(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 Switch0(config)#hostname S2
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption

En esta segunda parte se implementará la configuración de las VLAN, se definirán los puertos troncales y los de acceso igualmente se desactivarán las interfaces que no se utilizarán en el proyecto por temas de seguridad.

En un paso adicional se implementará en el Router el servicio de DHCP para a asignación de direccionamiento a los PC que se utilizaran durante las pruebas.

Los comandos se pueden ver en las tablas 3, 4 y 5

Tabla 3 Configuración de Vlan en S1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#channel-group 1 mode active S1(config-if)#channel-protocol lacp

Tabla 4 Configuración de Vlan en S2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config-if)#channel-group 1 mode active S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#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 S2(config)#interface range fa0/5-17 , fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Interfaces sin uso S2(config-if-range)#sh

Tabla 5 Configuración del Router R1.

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool DHCP-VLAN2 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool DHCP-VLAN3 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

En las imágenes siguientes se puede evidenciar que la configuracion del servicio DHCP fue correcta y ahoa tanto el PCA como el PCB estan tomando sus direcciones de forma correcta.

Figura 2 Configuración PCA

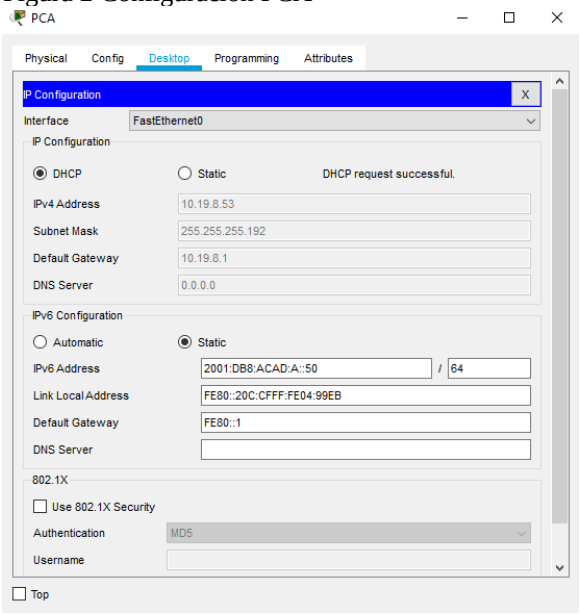
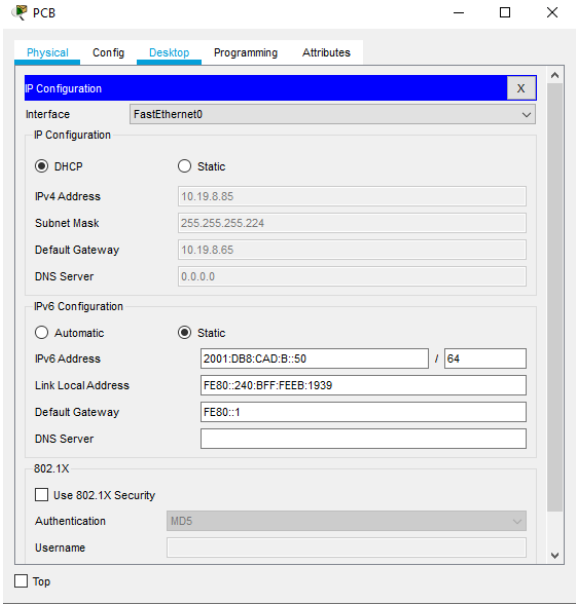


Figura 3 Configuración PCB



II. RESULTADOS

Luego de los pasos anteriores se realizan las verificaciones de conectividad entre dispositivos con el fin de identificar que las configuraciones aplicadas sean las correctas y la comunicación entre los dispositivos sea adecuada.

En la siguiente tabla se puede evidenciar por medio del comando ping tanto IPV4 como IPV6 en que casos se alcanza la conectividad:

Se verifica la contevidad via Ping entre los dispostivos y es satisfactoria, a continuacion en las figuras 4 y 5 se puede ver el resultado:

Figura 4

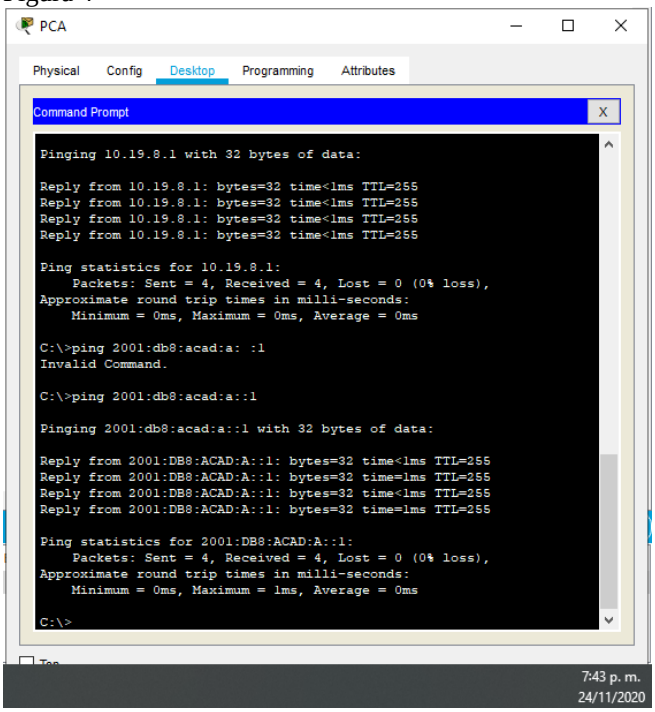
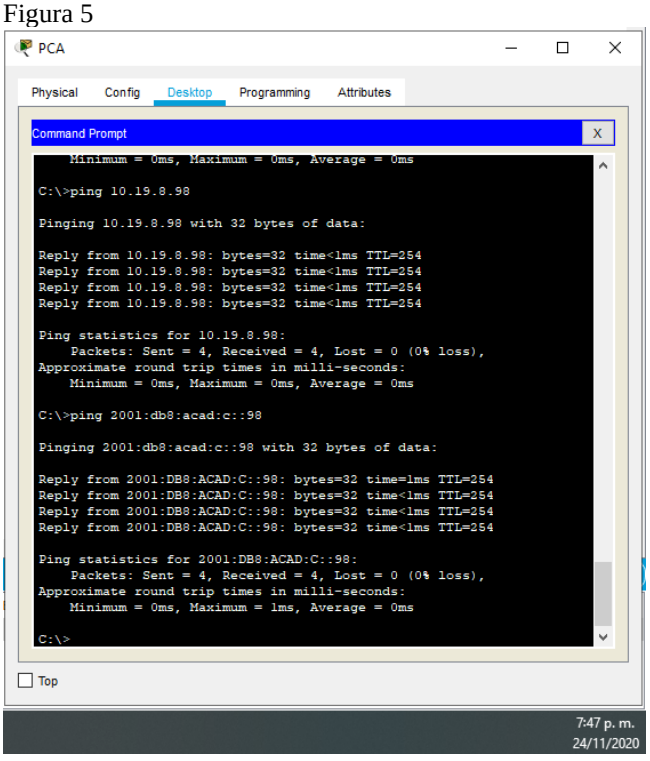


Figura 5



En este punto finalizan las pruebas de conectividad y alcance entre dispositivos.

III. CONCLUSIONES

Con el desarrollo de esta actividad de simulación se logró poner a prueba todos los conocimientos adquiridos durante el programa académico con la simulación de los escenarios propuestos.

En el escenario uno se trabajó prácticas que permitieron medir la destreza para implementar redes LAN segmentadas por VLAN, estas se aplicaron la configuración por cada puerto dependiendo de la funcionalidad seleccionada (Access, Trunk) igualmente se implementó entre los Switch Cisco el servicio de EtherChannel el cual nos permitió evidencia como se pueden definir mecanismos de seguridad en caso de fallas físicas de un puerto, así mismo se evidencio por medio de la practica la implementación de una red sobre IPV6 y las diferencias principales respecto a su antecesora IPV4

IV BIOGRAFIA

Wiler Velez, Nacio en Envigado antioquia el 09 de Junio del año 1987 pero se radico en el Valled del cauca desde los 7 años de edad se graduo de la Universidad Catolica Lumen Gentium como Tecnologo en Telecomunicaciones en el año 2014 y desde entonces su experiencia profesional se ha desarrollado en compañias de telecomunciones como Level 3, CenturyLink y Lumen.

IMPLEMENTACIO DE UN ESCENARIO PRACTICO UTILIZANDO LA HERRAMIENTA PACKET TRACER CON USO DE TECNOLOGÍA CISCO

Wilfer Velez Orozco
Universidad Nacional Abierta y a Distancia UNAD, velezo@unadvirtual.edu.co

Resumen

Por medio de la modalidad de "Proyecto Aplicado" el cual es desarrollado sobre un ambiente de simulación en Packet Tracer, herramienta de propiedad del gigantesco fabricante de dispositivos comunicaciones CISCO y que permite a los estudiantes de telecomunicaciones simular entornos prácticamente similares a los que se enfrentarían con equipos físicos reales.

Inicialmente se definen los elementos con los cuales se realizará la práctica, en este punto se deberán elegir los mas adecuados y que se ajusten según los requerimientos del ejercicio planteado.

La temática elegida en el curso CNNA que se abordaran durante el desarrollo del escenario son los siguientes: análisis inicial del diagrama propuesto, análisis de las tablas de direccionamiento y tabla de VLANs, posteriormente se configuraran los parámetros básicos en los dispositivos como la seguridad, los nombres así mismo los parámetros IP en las interfaces, en la siguiente etapa se implementaran las VLAN, se asignaran los puertos de acceso y troncales por último el EtherChannel.

En la fase final se habilitará desde el Router el protocolo DHCP y se deberá probará conectividad entre todos los dispositivos.

Palabras claves: **CISCO, LAN, WAN, VLAN, DHCP, EherChannel**

***Abstract*:**
Through the Applied project modality which is developed on a simulation environment in Packet Tracer, a tool owned by the giant manufacturer of communications devices CISCO and that allows telecommunications students to simulate environments practically similar to those they would face with equipment real physicists.

Initially the elements with which the practice will be carried out are defined, at this point the most appropriate ones must be chosen and adjusted according to the requirements of the proposed exercise.

The topics chosen in the CNNA course that will be addressed during the development of the scenario are the following: initial analysis of the proposed diagram, analysis of the addressing tables and VLANs table, later the basic parameters will be configured in the devices such as security, Also names the IP parameters in the interfaces, in the next stage the VLANs will be implemented, the access ports and trunks will be assigned finally the EtherChannel.

In the final phase, the DHCP protocol will be enabled from the Router and connectivity between all devices must be tested.

Keywords: **CISCO, LAN, WAN, VLAN, DHCP EtherChannel**

I. INTRODUCCION

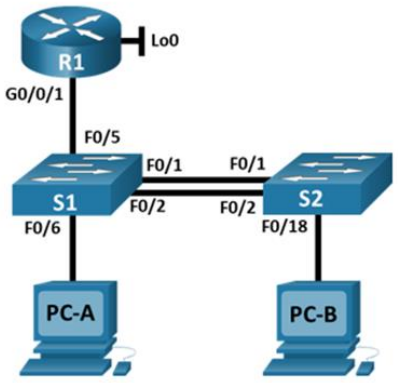
En la actualidad las comunicaciones se han convertido en parte fundamental de la operación en de casi cada dispositivo electrónico, el internet de las cosas llego para quedarse tanto en los ambientes familiares como empresariales por esta razón cada vez es común ver como la demanda de personas expertas en la implementación de redes de comunicaciones que integren deferentes aspectos como la escalabilidad, la seguridad la convergencia y a su vez que los diseños sean lo mas optimizados posibles para tener costos razonables.

METODOLOGIA

Se plantea un escenario en la figura 1 en el cual con la estructura de la red y las tablas de direccionamiento y VLANs se deberá implementar sobre la herramienta Packet Tracer el esquema que se mencionó anteriormente

El resultado final será garantizar el correcto funcionamiento de la red, la conectividad entre los dispositivos y la asignación de direccionamiento IP para cada una de las VLAN desde el router via DHCP

Topología de red escenario 1



Lista de direccionamiento IP

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

Lista de Vlans

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

Se da inicio con la inicialización de los dispositivos, estos comprenden el borrado de la configuración almacenadas en la memoria interna y las tablas de VLAN, se activa la configuración de la plantilla SDM para la admisión de IPv6.

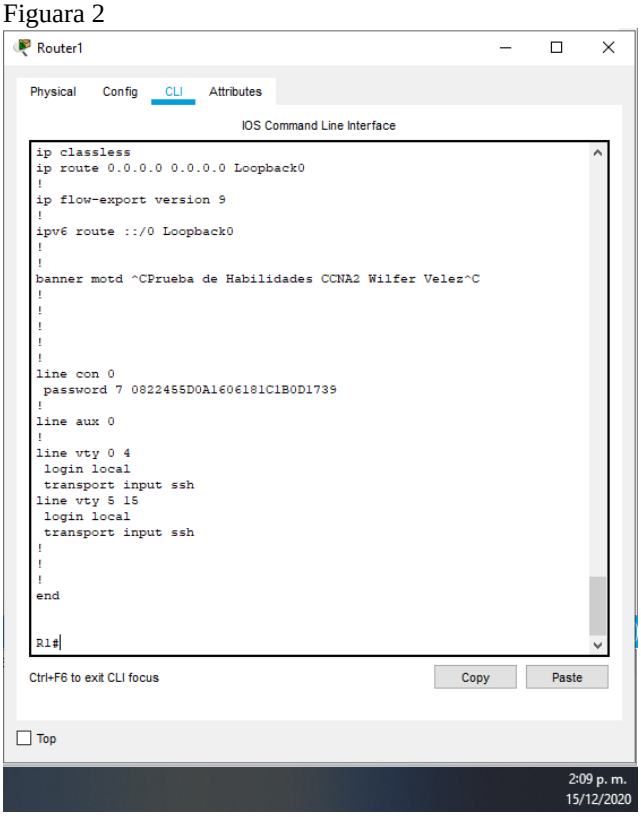
Posteriormente se realiza la implementación de los elementos básicos como son la seguridad de los dispositivos, los accesos remotos permitidos, la configuración IPV4 e IPV6 de las interfaces y las rutas por defecto, los comandos ejecutados se presentan en las Tablas 1 y 2

Tabla 1
Configurar R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#conf terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Escenario 1 Ivan Caro R1"
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

En la siguiente figura se puede evidenciar la configuración aplicada sobre el Router 1 en la cual vemos el banner y los parámetros de seguridad aplicados sobre las líneas de consola y VTY

Figuara 2



A continuación en la tabla 2 realizamos la configuración inicial de los SW

Tabla 2 Configurar los Switch S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup Switch0(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 Switch0(config)#hostname S2
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config-line)#password ciscoconpass S2(config-line)#password ciscoconpass
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S2(config)#service password-encryption

En esta segunda parte se implementará la configuración de las VLAN, se definirán los puertos troncales y los de acceso igualmente se desactivarán las interfaces que no se utilizarán en el proyecto por temas de seguridad.

En un paso adicional se implementará en el Router el servicio de DHCP para a asignación de direccionamiento a los PC que se utilizaran durante las pruebas.

Los comandos se pueden ver en las tablas 3, 4 y 5

Tabla 3 Configuración de Vlan en S1

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#channel-group 1 mode active S1(config-if)#channel-protocol lacp

Tabla 4 Configuración de Vlan en S2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config-if)#channel-group 1 mode active S2(config-if)#channel-protocol lacp
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#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 S2(config)#interface range fa0/5-17 , fa0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Interfaces sin uso S2(config-if-range)#sh

En la siguiente figura se puede evidenciar en el SW1 la configuración aplicada para habilitar las VLAN solicitadas en el ejercicio

Figura 2 Resultado configuración Vlan

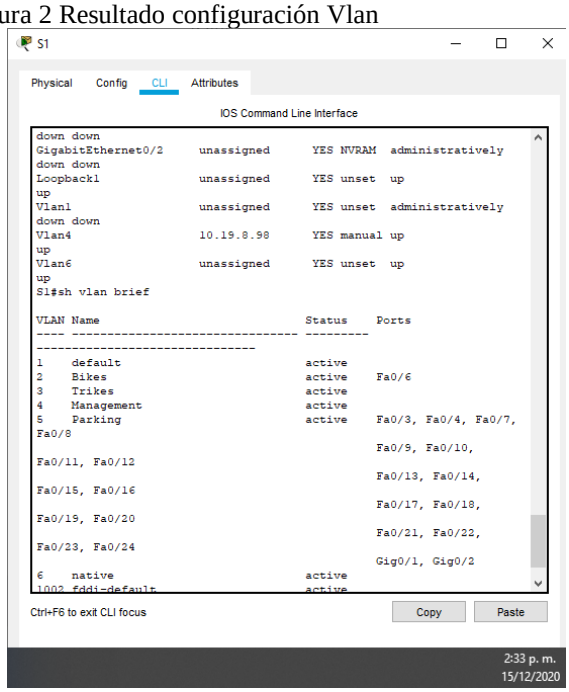
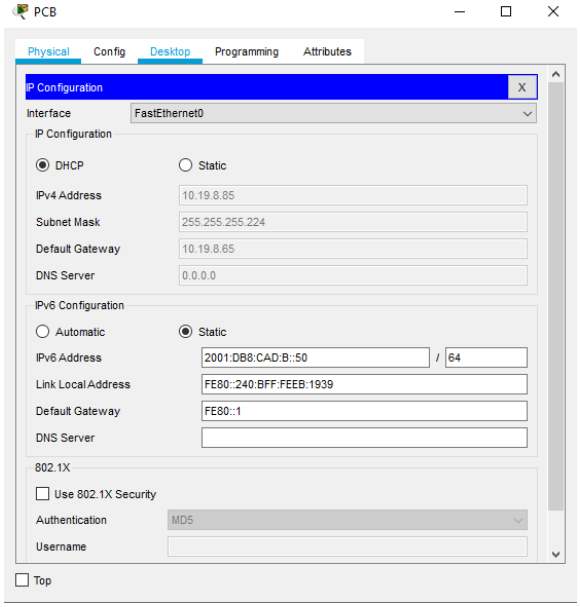


Figura 3 Configuración PCB



II. RESULTADOS

Tabla 5 Configuración del Router R1.

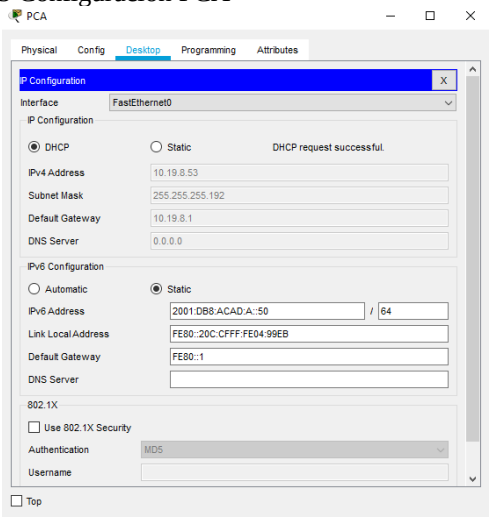
Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool DHCP-VLAN3 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

Luego de los pasos anteriores se realizan las verificaciones de conectividad entre dispositivos con el fin de identificar que las configuraciones aplicadas sean las correctas y la comunicación entre los dispositivos sea adecuada.

En las imágenes siguientes se puede evidenciar que la configuracion del servicio DHCP fue correcta y ahoa tanto el PCA como el PCB estan tomando sus direcciones de forma correcta.

En la siguiente tabla se puede evidenciar por medio del comando ping tanto IPV4 como IPV6 en que casos se alcanza la conectividad:

Figura 3 Configuración PCA



Se verifica la contevidad via Ping entre los dispostivos y es satisfactoria, a continuacion en las figuras 4 y 5 se puede ver el resultado:

Figura 4 Resultado Ping

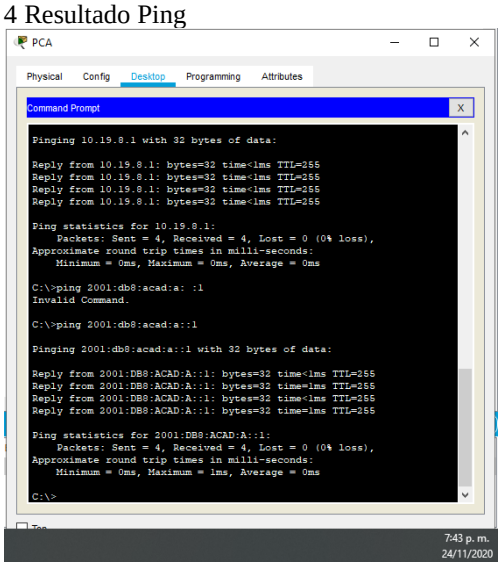
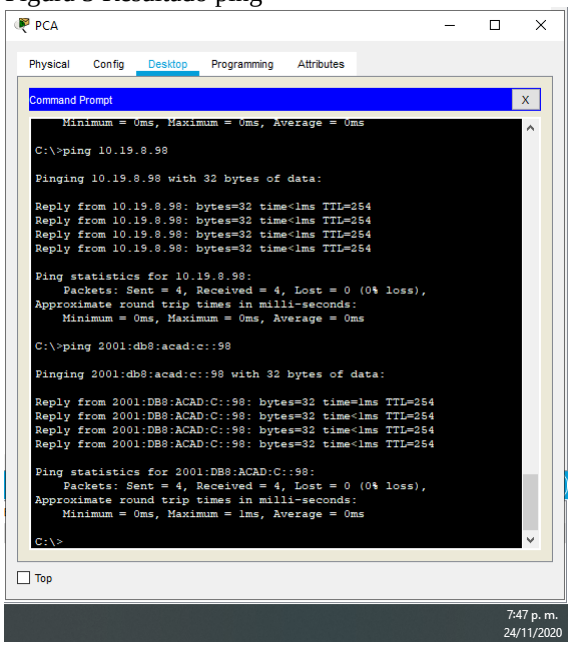


Figura 5 Resultado ping



En este punto finalizan las pruebas de conectividad y alcance entre dispositivos.

III. CONCLUSIONES

Con el desarrollo de esta actividad de simulación se logró poner a prueba todos los conocimientos adquiridos durante el programa académico con la simulación de los escenarios propuestos.

En el escenario uno se trabajó prácticas que permitieron medir la destreza para implementar redes LAN segmentadas por VLAN, estas se aplicaron la configuración por cada puerto dependiendo de la funcionalidad seleccionada (Access, Trunk) igualmente se implementó entre los Switch Cisco el servicio de EtherChannel el cual nos permitió evidencia como se pueden definir mecanismos de seguridad en caso de fallas físicas de un puerto, así mismo se evidencio por medio de la practica la implementación de una red sobre IPV6 y las diferencias principales respecto a su antecesora IPV4

IV BIOGRAFIA

Wiler Velez, Nacio en Envigado antioquia el 09 de Junio del año 1987 pero se radico en el Valled del cauca desde los 7 años de edad se graduo de la Universidad Catolica Lumen Gentium como Tecnologo en Telecomunicaciones en el año 2014 y desde entonces su experiencia profesional se ha desarrollado en compañias de telecomunciones como Level 3, CenturyLink y Lumen.