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

FABIAN CAMILO ALVARADO SANABRIA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
BUCARAMANGA
2020

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

FABIAN CAMILO ALVARADO SANABRIA

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

DIRECTOR:
DIEGO EDINSON RAMÍREZ CLAROS
MASTER EN GERENCIA DE PROYECTO DE TELECOMUNICACIONES

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BUCARAMANGA
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bucaramanga, 17 de noviembre de 2020

AGRADECIMIENTOS

Mi agradecimiento primeramente está dirigido a Dios, quien me dio la oportunidad y salud de hacer este sueño realidad, agradezco a mi familia, quienes me apoyaron incondicionalmente en todos y cada uno de los retos que he superado en mi proyecto de estudios universitarios.

Agradezco a todas las personas y maestros, que durante mi proceso de formación me compartieron su conocimiento y sabiduría, que gracias a su apoyo incondicional hicieron que este proyecto de estudios fuera un logro más en mi vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

INTERFACE**:** se denota como interface a todo conector físico y lógico, cuyo propósito principal es enviar y recibir paquetes de información. Las propiedades de las interfaces pueden ser modificadas por el usuario para garantizar la conectividad entre dos o más interfaces de un dispositivo de red.

LOOPBACK: se usa para llamar todas aquellas interfaces virtuales que pueden ser creadas por el usuario, para fines particulares de su diseño.

NOMBRE DE DOMINIO: es un nombre único utilizado por personas o entidades en la red de Internet, cuyo propósito es el de identificar de manera exclusiva sus sitios en la web.

IPV6: es la versión número 6 del protocolo de internet, que mediante sus 340 sextillones de IP's, hacen posible la identificación única de todos los dispositivos en la red.

VTY: son las líneas de terminal virtual del dispositivo, que se utilizan para habilitar las conexiones de usuarios a través del protocolo telnet con el propósito de realizar su gestión remota.

OSPF: es un protocolo de enrutamiento dinámico, cuya función principal consiste en orientar el tráfico por la ruta más rápida, su elección de ruta está basada principalmente en enlaces con mejor ancho de banda y baja congestión.

PING: es una herramienta para el diagnóstico de redes, en la que se realiza el envío de paquetes ICMP con el fin de determinar la conectividad entre dispositivos.

RESUMEN

Durante la ejecución de las practicas del diplomado CCNA de Cisco, habremos adquirido destrezas y conocimientos para la configuración global de dispositivos de red tales como Reuters y switches. En las practicas se ejecutan comandos básicos y avanzados para la configuración de interfaces de red, a fin de habilitar la comunicación y respuesta de todos los dispositivos que conforman la red.

Es importante destacar, que se utilizara el direccionamiento y enrutamiento para IPV6, cuya finalidad es sustituir su anterior versión 4, para lo cual se abordaran los comandos y consideraciones para tal fin. Al final del desarrollo de las prácticas, tendremos una clara perspectiva de los requerimientos y condiciones que debe cumplir cada de los dispositivos; para lograr la integración de protocolos y características de las redes de nueva generación.

Finalmente, se ejecutarán configuraciones de enrutamiento dinámico y estático, en las que se observarán cada uno de sus parámetros básicos para establecer el enrutamiento entre dispositivos. Como actividad adiciona, se configurarán listas de acceso para el control de accesos desde dispositivos no deseados, lo que facilita la seguridad en la gestión de dispositivos de red.

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

ABSTRACT

During the execution of the practices of the Cisco CCNA diploma, we will have acquired skills and knowledge for the global configuration of network devices such as Reuters and switches. In the practices, basic and advanced commands are executed for the configuration of network interfaces, in order to enable communication and response from all the devices that make up the network.

It is important to note that addressing and routing for IPV6 will be used, the purpose of which is to replace its previous version 4, for which the commands and considerations for this purpose will be addressed. At the end of the development of the practices, we will have a clear perspective of the requirements and conditions that each of the devices must meet; to achieve the integration of protocols and characteristics of the next generation networks.

Finally, dynamic and static routing configurations will be executed, in which each of its basic parameters will be observed to establish the routing between devices. As an additional activity, access lists will be configured to control access from unwanted devices, which facilitates security in the management of network devices.

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

INTRODUCCIÓN

Durante el desarrollo del presente informe se realizaran prácticas en las que se configuraran características propias del dispositivo, configuración de protocolos, y pruebas de funcionamiento y conectividad de dispositivos de la marca cisco, la temática estará compuesta por uso de comandos básicos para la configuración de dispositivos, en los que se mostrara la manera del como configurar temas relacionados seguridad, acceso remoto al dispositivo, rutas, nombramiento e identificación personalizada del dispositivo; a fin de reconocerlos y gestionarlos de manera adecuada.

Por otra parte, mediante el uso del simulador de redes de cisco, el cual es conocido con el nombre de Packet Tracer, desarrollaremos las practicas propuestas en los escenarios de habilidades del diplomado CCNA, en dichas prácticas se tratarán conceptos tales como conexión y diseño de la topología, elección de medios físicos para la comunicación, configuración y uso de interfaces, asignación de sus respectivas IP para la identificación y uso de enrutamiento. En cuanto a las pruebas, se dará uso de herramientas para la verificación de conectividad tales como Ping, Traceroute, Ipconfig, entre otros.

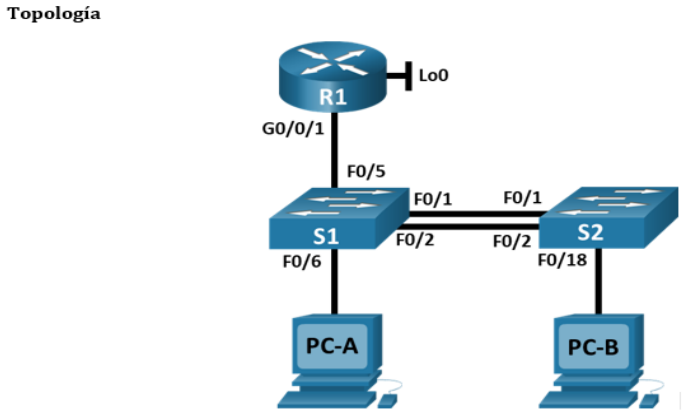
Finalmente, se ejecutarán prácticas que permitirán configurar y entender el enrutamiento de dispositivos de capa 3, mediante la ejecución de la práctica se conocerán las sentencias para establecer un enrutamiento estático y dinámico según sea la preferencia del usuario. Adicionalmente se establecerán listas de acceso para el control de acceso; lo que ayudara a fortalecer los aspectos de seguridad en los dispositivos de red.

1. DESARROLLO

1.1. ESCENARIO 1

En el primer escenario se plantea la configuración de dispositivos de una red pequeña. Para ello se debe configurar un Router y dos Switches que permitan la conectividad IPv4 e IPv6 para los hosts conectados. El Reuter y los switches deben administrarse de forma segura. Se deberá configurar el enrutamiento entre las diferentes redes asignadas en el escenario, para ello debe usar los conceptos de VLAN, DHCP, EtherChannel y port-security.

Figura 1. Topología de Escenario 1



A continuación, se describen todas y cada una de la Vlan que deben ser configuradas en los dispositivos que integran la red.

Tabla 1. Vlans de red propuesta

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

Fuente: Autor

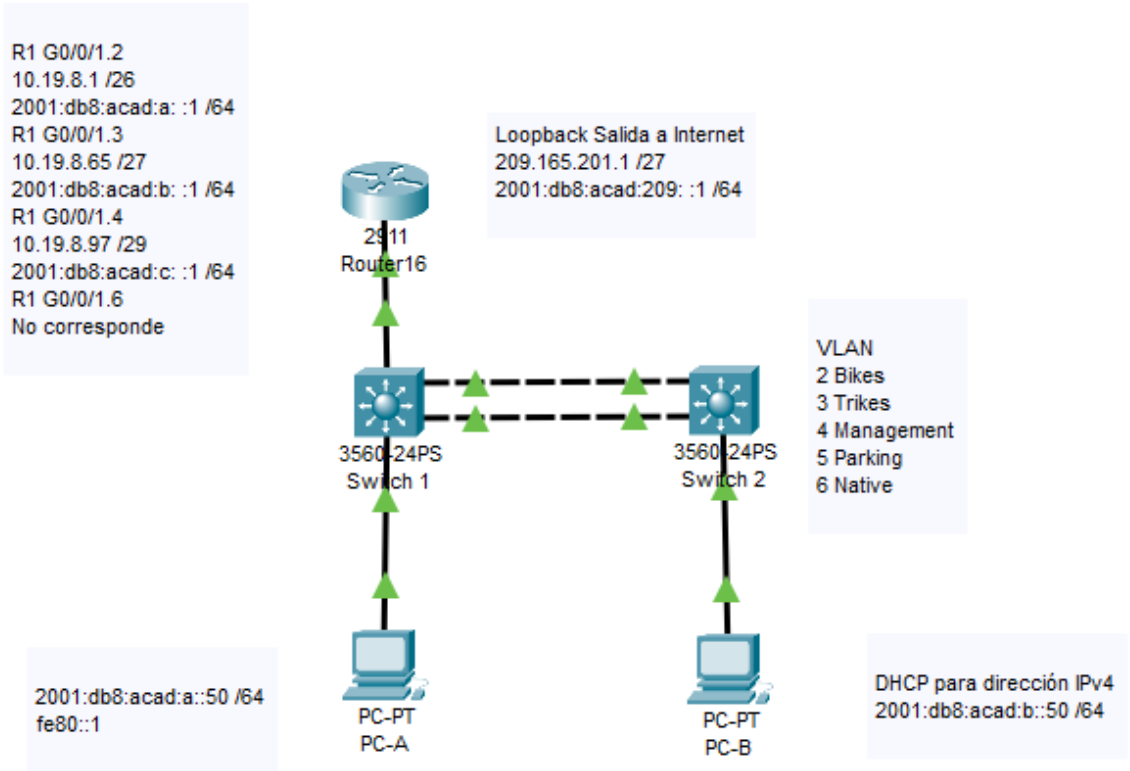
A continuación, se listan el direccionamiento para cada una de las interfaces y equipos utilizados en el escenario 1.

Tabla 2. Direccionamiento de Interfaces

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Fuente: Autor

Figura 2. Simulación montada en Packet Tracer



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

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

Después de realizar la selección y conexión de los dispositivos de red a utilizar, procedemos como primera medida a efectuar el clareo o borrado de las configuraciones que pueden tener de forma predeterminada los dispositivos, entre las más comunes se encuentran listados de VLAN por defecto y configuraciones interfaces que puedan existir.

Para ello usamos los siguientes comandos a fin de que los dispositivos queden sin ninguna configuración, que pueda afectar el desarrollo de la actividad del escenario 1:

Tabla 3. Comandos para inicializar router

Comando	Función
Router>enable	Comando para ingreso a modo Exec privilegiado
Router#erase startup-config	Comando para borrar la configuración inicial del dispositivo
Router#reload	Comando para reiniciar el dispositivo

Fuente: Autor

Tabla 4. Comandos para inicializar switch

Comando	Función
Switch>enable	Comando para ingreso a modo Exec privilegiado
Switch#erase startup-config	Comando para borrar la configuración inicial del dispositivo
Switch#delete vlan.dat	Comando para borrar la bd de vlan existentes en el dispositivo
Switch#reload	Comando para reiniciar el dispositivo

Fuente: Autor

Con el fin de que los swhiches permitan el uso de direccionamiento IPV6, es necesario efectuar el cambio de la plantilla SDM, dicha plantilla hace referencia a una configuración que el usuario establece a fin de aprovechar al máximo los recursos del dispositivo para los fines que el usuario a bien tenga. Es importante saber, que de manera predeterminada los swhitches no permiten el direccionamiento ipv6 en sus interfaces, para lo cual aplicamos el siguiente comando para que sea habilitada esta característica en los dispositivos:

Tabla 5. Comandos para configuración de plantilla SMD

Comando	Función
Switch>enable	Comando para ingreso a modo Exec privilegiado
Switch#configure terminal	Comando para ingreso a modo Exec de configuración global
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default	comando para habilitar el direccionamiento ipv6 e ipv4 en el dispositivo
Switch(config)#reload	comando para reiniciar el dispositivo

Fuente: Autor

Paso 2 Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:
Para ello señalaremos todos los comandos para logar la configuración solicitada.

Tabla 6. Paso 2 Router 1

Tarea	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	R1 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)#line console 0 R1(config-line)#password ciscoenpass R1(config-line)#login
Contraseña de acceso a la consola: **ciscoconpass**	R1(config)#enable password ciscoconpass
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 R1(config-line)#exit
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 #el acceso a este dispositivo esta administrado y regulado por Fabian camilo alvarado#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces: Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	R1(config)# interface GigabitEthernet0/1 R1(config-if)#description Interface de router R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown R1(config-if)#exit R1(config)# interface GigabitEthernet0/1.2 R1(config-subif)#description Bikes R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:DB8:ACAD:A::1/64 R1(config-subif)#exit R1(config)# interface GigabitEthernet0/1.3 R1(config-subif)#description Trikes R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:DB8:ACAD:B::1/64

	R1(config-subif)# ipv6 address FE80::1 link-local R1(config-subif)#exit R1(config)#interface GigabitEthernet0/1.4 R1(config-subif)#description Management R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:DB8:ACAD:C::1/64 R1(config-subif)#exit R1(config)#interface GigabitEthernet0/1.6 R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#exit
Configure el Loopback0 interface: Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**	R1(config)#int l0 R1(config-if)#description Salida de Internet R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate Rsa general-keys modulus 1024

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 1 cuente con los parámetros básicos seguridad, en adelante solicitara contraseña para el acceso a través de consola, al igual, que solicitara usuario y contraseña para el ingreso remoto a través del protocolo de seguridad SSH. Por otra parte, se crearon las subinterfaces a las cuales se les asignaron las direcciones IP de cada red mediante el protocolo IEEE 802.1Q; y que en adelante estas estarán funcionado de manera simultánea sobre la misma interfaz física.

Paso 3 Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 7. Paso 3 Switch 1 y 2

Tarea	Especificación
Desactivar la búsqueda DNS.	Swith(config)# no ip domain-lookup
Nombre del switch: **S1 o S2, según proceda**	Swith(config)#hostmane S1 S1(config)#exit Swith(config)#hostmane S2 S2(config)#exit
Nombre de dominio: **ccna-lab.com**	S1(config)# ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado: **Ciscoenpass**	S1(config)#enable password ciscoenpass
Contraseña de acceso a la consola: **Ciscoconpass**	S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login
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 S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#S1(config-line)#transport input ssh S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #ESTA DISPOSITIVO ES ADMINISTRADO Y REGULADO POR FABIAN CAMILO ALVARADO#
Generar una clave de cifrado RSA **Módulo de 1024 bits**	S1(config)#crypto key generate Rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2**	**S1** Establecer la dirección IPv6 de capa 3 S1(config)#int vl 4 S1(config-if)#Description Management S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit S1(config)#ipv6 route ::/0 2001:db8:acad:c::1 **S2** S2(config)#int vl 4 S2(config-if)#Description Management S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit S2(config)#ipv6 route ::/0 2001:db8:acad:c::1

Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S2(config)#ip default-gateway 10.19.8.97

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que los switches 1 y 2 cuenten con los parámetros básicos seguridad, en adelante solicitara contraseña para el acceso a través de consola, al igual que solicitara usuario y contraseña para el ingreso remoto a través del protocolo de seguridad SSH. Por otra parte, se configuraron cada una de las interfaces Vlan que en adelante servirán como puertos de gestión de los dispositivos en los que se podrá acceder por IPv4 e IPv6.

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

Paso 4 Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 8. Paso 4 Configuración Switch 1

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config)#int vl 2 S1(config-vlan)#description Bikes S1(config-if)#exit S1(config)#int vl 3 S1(config-vlan)#description Trikes S1(config-if)#exit S1(config)#int vl 4 S1(config-vlan)#description Management S1(config-if)#exit S1(config)#int vl 5 S1(config-vlan)#description Parking S1(config-if)#exit S1(config)#int vl 6 S1(config-vlan)#description Native S1(config-if)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#int fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#int fastEthernet 0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit S1(config)#int fastEthernet 0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
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)#interface range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#exit
Configurar el puerto de acceso de host para VLAN 2	S1(config)#int f0/6 S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1(config)#int f0/6 S1(config-if)#switchport port-security max S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas, Asigne la VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#interface range f0/3-4 S1(config-if-range)#switchport mode access vl 5 S1(config-if-range)#description inutilizados

	S1(config-if-range)#shutdown S1(config)#interface range f0/7-24 S1(config-if-range)#switchport access vl 5 S1(config-if-range)#shutdown

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el switch 1 tenga listadas y nombradas cada una de las Vlan que operan en la red, por otro lado, se ha configurado los puertos Fe0/1 Y Fe0/2 como puertos troncales, los cuales permitieran el tráfico encapsulado mediante un EtherChannel que usa el protocolo LACP para agregación de conexiones virtuales. Por último, se deja configuradas cada una de las interfaces del dispositivo con su respectiva Vlan de acceso, también se dejan inactivos todos los puertos que no tienen función en la red.

Paso 5 Configure el S2

Entre las tareas de configuración de S2 se incluyen las siguientes:
Tabla 9. Configuración Switch 2

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config)#int vl 2 S2(config-vlan)#description Bikes S2(config-if)#exit S2(config)#int vl 3 S2(config-vlan)#description Trikes S2(config-if)#exit S2(config)#int vl 4 S2(config-vlan)#description Management S2(config-if)#exit S2(config)#int vl 5 S2(config-vlan)#description Parking S2(config-if)#exit S2(config)#int vl 6 S2(config-vlan)#description Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#int fastEthernet 0/1

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 S2(config-if)#exit S2(config)#int fastEthernet 0/2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit
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)#interface range fastEthernet 0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if)#switchport trunk native vlan 6 S2(config-if-range)#exit
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#Interfaz F0/18 S2(config-if)#interface FastEthernet0/18 S2(config-if)#switchport access vlan 3 S2(config-if)#switchport mode access
Configure port-security en los access ports permite 3 MAC addresses	S2(config)#Interfaz F0/18 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 f0/3-17 S2(config-if-range)#switchport mode access vl 5 S2(config-if-range)#description inutilizados S2(config-if-range)#shutdown S2(config)#interface range f0/19-24 S2(config-if-range)#switchport access vl 5 S2(config-if-range)#shutdown

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el switch 2 tenga listadas y nombradas cada una de las Vlan que operan en la red, por otro lado, se ha configurado los puertos Fe0/1 Y Fe0/2 como puertos troncales, los cuales permitieran el tráfico encapsulado mediante un EtherChannel que usa el protocolo LACP para agregación de conexiones virtuales. Por último, se deja configuradas cada una de las interfaces del dispositivo con su respectiva Vlan de acceso, también se dejan inactivos todos los puertos que no tienen función en la red.

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10. Parámetros enrutamiento Router 1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ipv6 route ::/0 loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 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 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(dhcp-config)#exit 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 ccna-a.net R1(dhcp-config)#network 10.19.8.64 255.255.255.224

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(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

Fuente: Autor

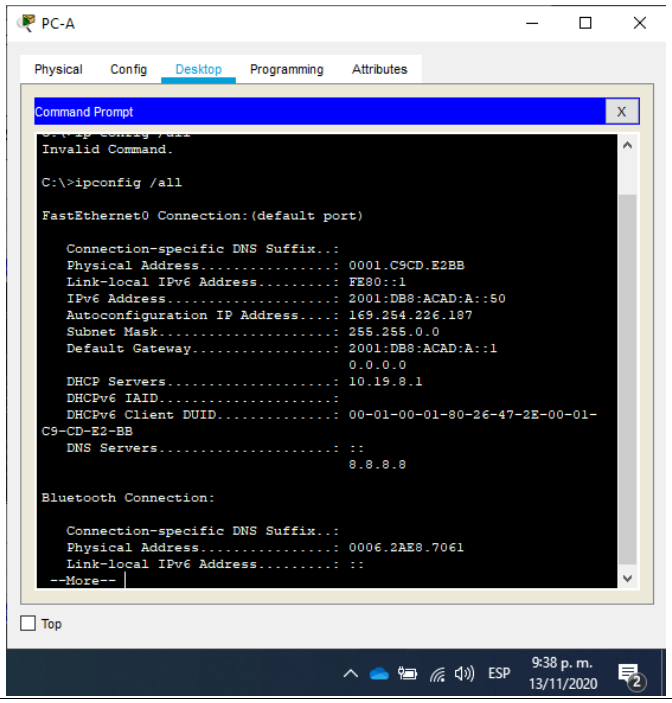
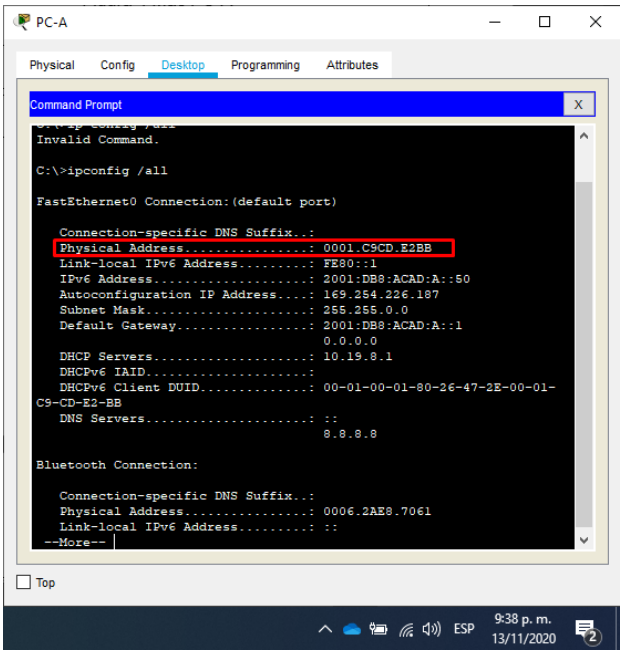
Al haber aplicado los comandos anteriores, se logra que el router 1 asigne dirección IP a los hosts mediante la activación del servicio de DHCP, esta configuración excluirá un rango de 10 IP's para cada uno de los rangos configurados, por otra parte, la asignación de direccionamiento dependerá del puerto al que está conectado el host y a la vlan que este permita dicho puerto. Finalmente, fueron asignadas las rutas estáticas que simularan la salida a Internet, ya que todo trafico que no refiera a alguna de las direcciones configurada en la red, esta será transmitida por loopback 0 quien hará las veces de conectividad a la red de Internet.

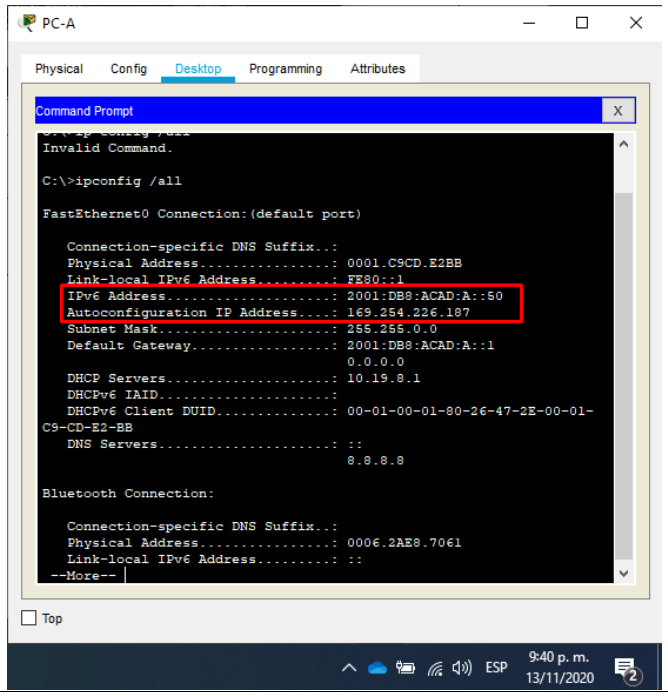
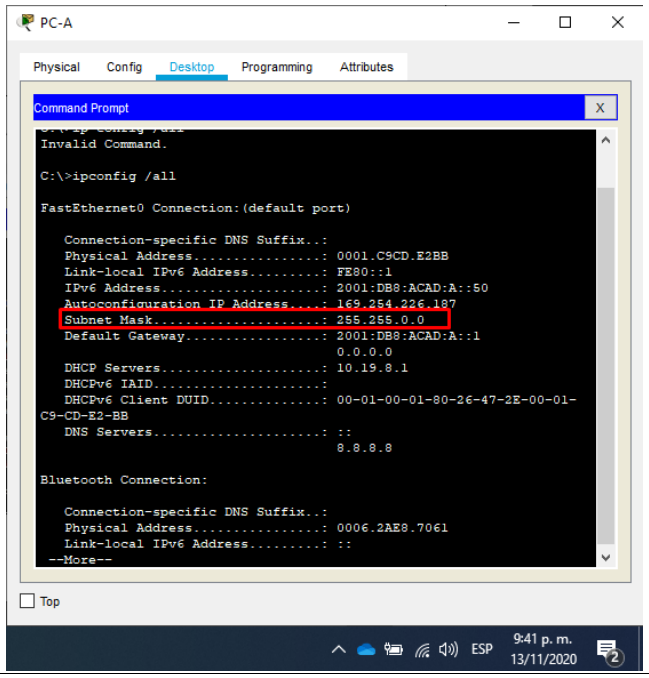
Paso 2 Configurar los servidores

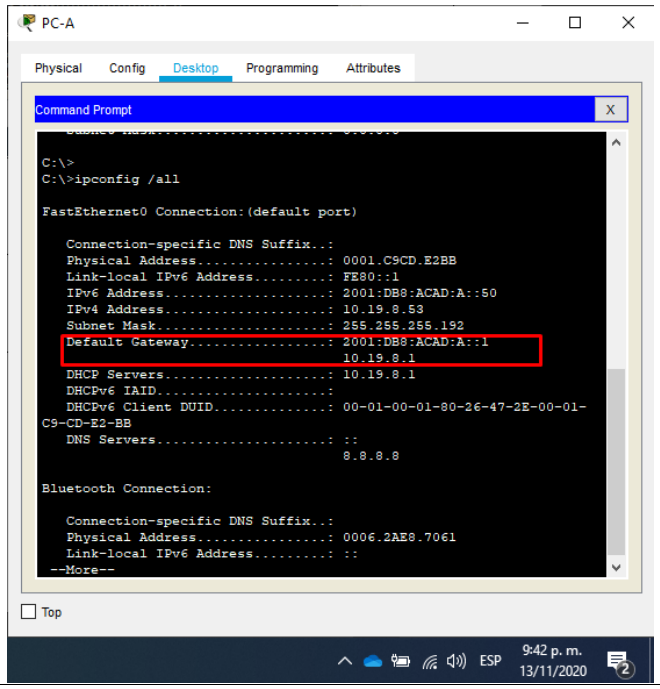
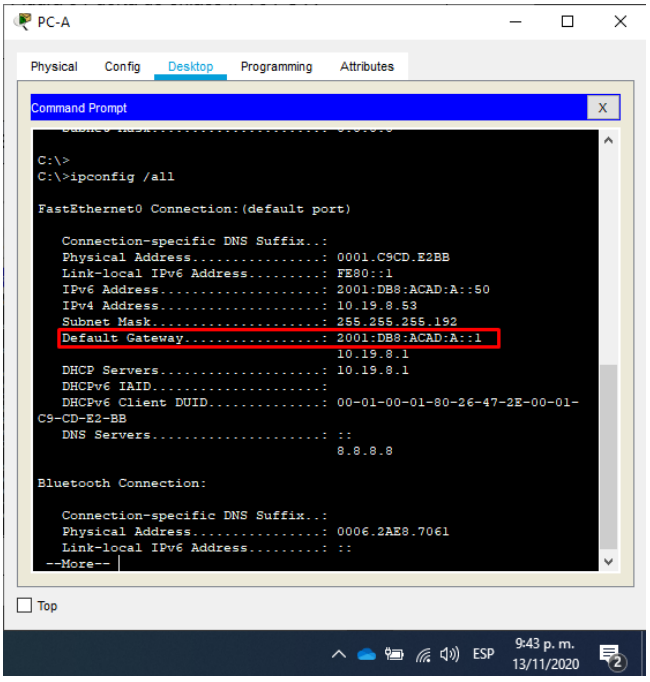
Realice la configuración de los equipos host PC-A y PC-B para que reciban direccionamiento mediante DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

A continuación, se ilustrará cada una cada una de las configuraciones de red que debe tener cada uno de los dispositivos en su tarjeta de red, así mismo, la descripción de todos los parámetros de la misma, en los que se encuentra la dirección IPv4 e IPv6, dirección MAC, mascará de red para IPv4, Link local para IPv6 y su respectiva puerta de enlace.

Tabla 11. Evidencias de configuración de red PC-A

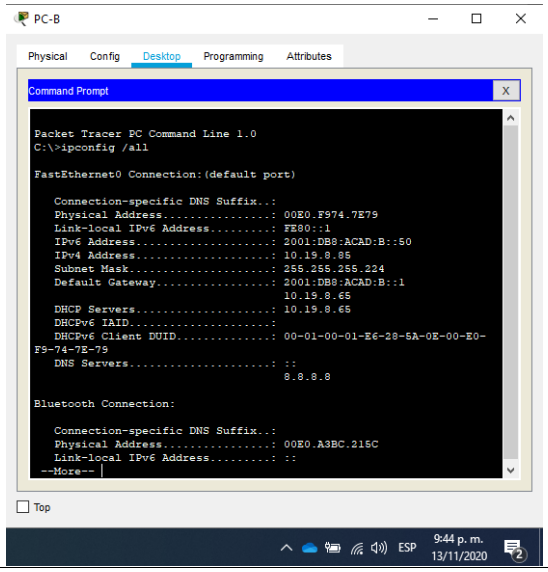
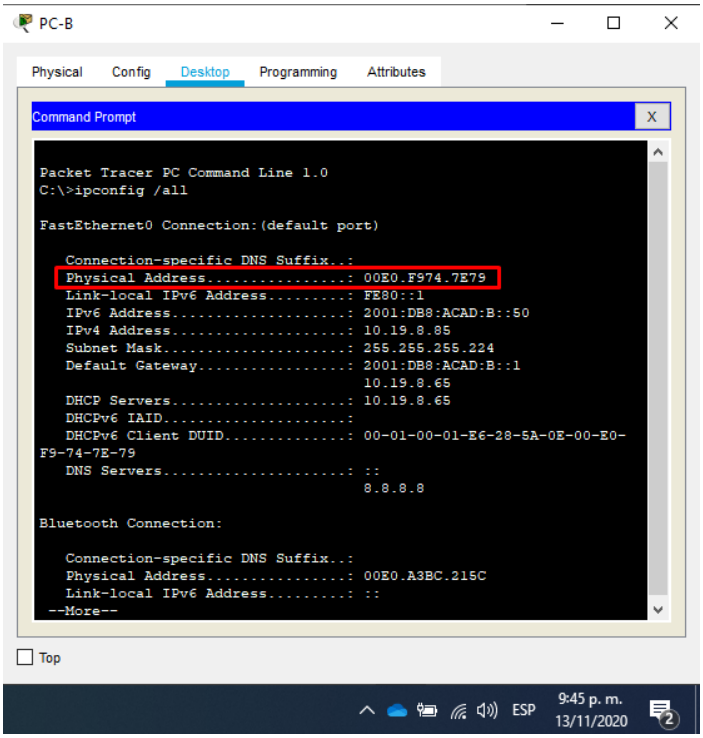
CONFIGURACIÓN DE RED PC-A	
Parámetros de red PC-A	Figura 3. Parámetros de red PC-A 
Mac PC-A	Figura 4. Mac PC-A 

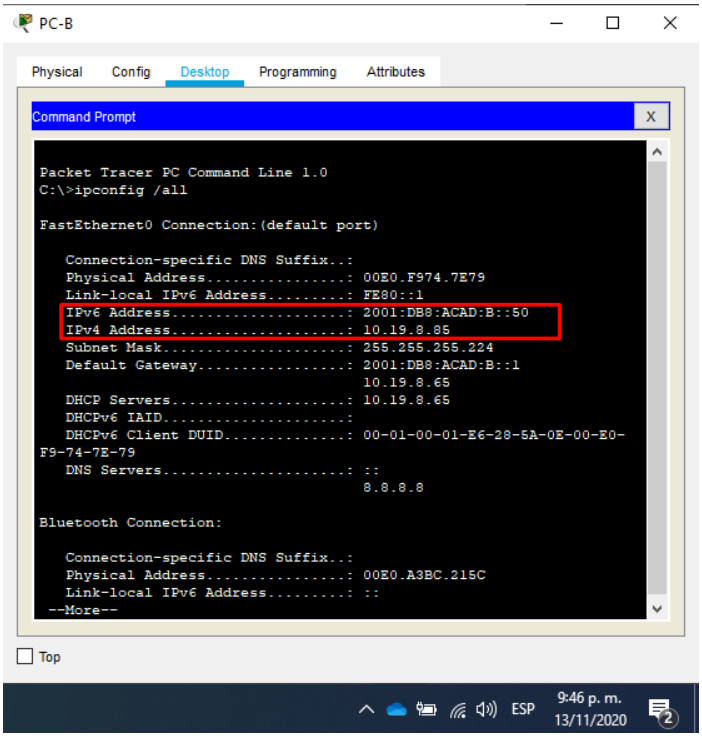
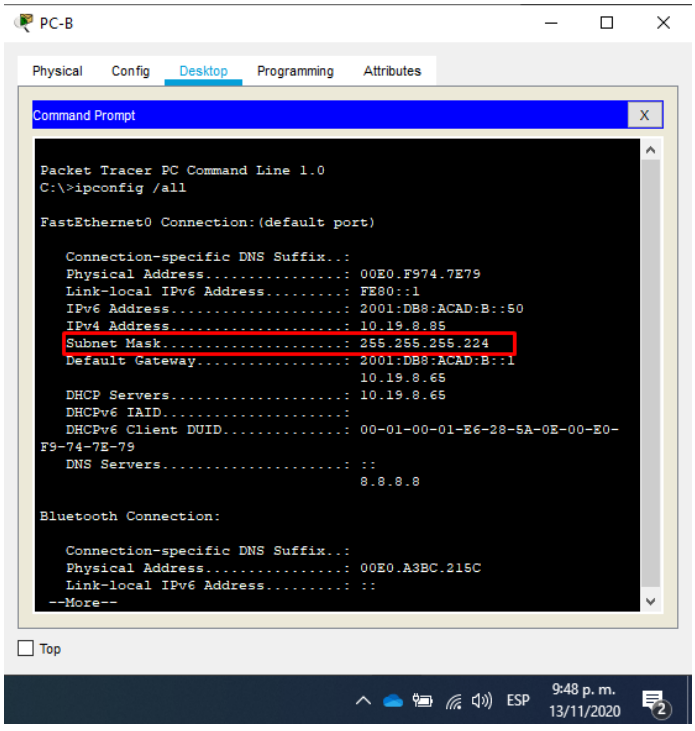
Dirección IPV4 e IPV6 de PC-A	Figura 5. Dirección IPV4 e IPV6 de PC-A 
Mascara de red PC-A	Figura 6. Mascara de red PC-A 

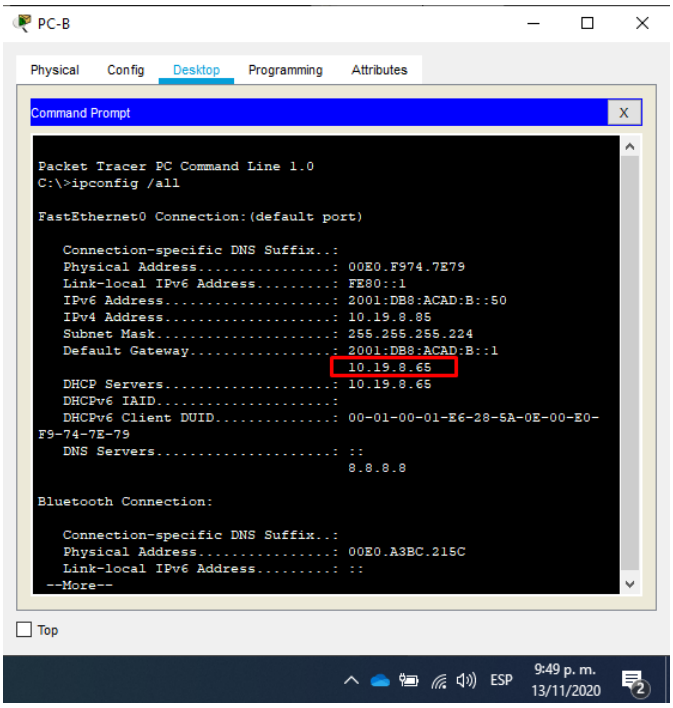
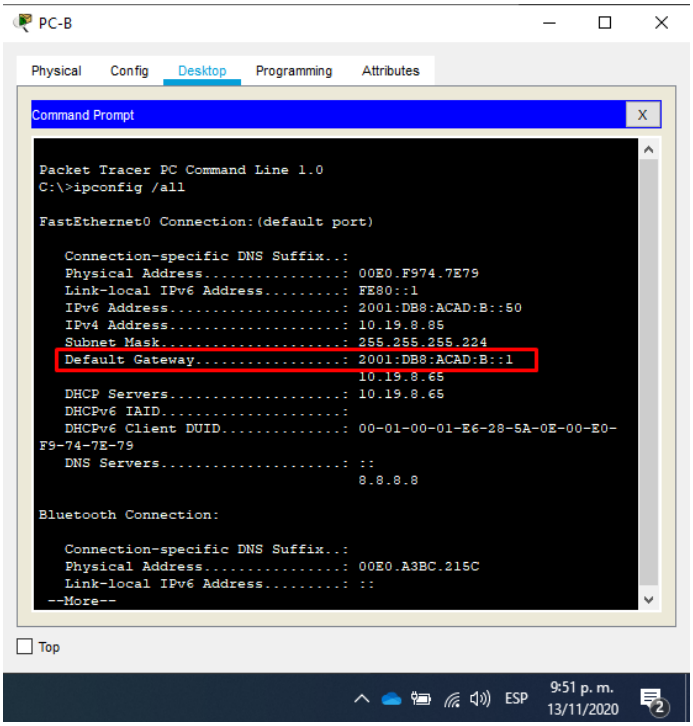
Puerta de enlace IPV4 PC-A	Figura 7. Puerta de enlace IPV4 PC-A 
Puerta de enlace IPV6 PC-A	Figura 8. Puerta de enlace IPV6 PC-A 

Fuente: Autor

Tabla 12. Evidencias de configuración de red PC-B

CONFIGURACIÓN DE RED PC-B	
Parámetros de red PC-B	Figura 9. Parámetros de red PC-B 
Mac PC-B	Figura 10. Mac PC-B 

Dirección IPV4 e IPV6 de PC-B	Figura 11. Dirección IPV4 e IPV6 de PC-B 
Mascara de red PC-B	Figura 12. Mascara de red PC-B 

Puerta de enlace IPV4 PC-A	Figura 13. Puerta de enlace IPV4 PC-A 
Puerta de enlace IPV6 PC-B	Figura 14. Puerta de enlace IPV6 PC-B 

Fuente: Autor

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

Se utilizará herramienta de ping para probar la conectividad a nivel de direccionamiento IPv4 e IPv6 entre todos los equipos de red.

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

Tabla 13. Pruebas de conectividad de dispositivos

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

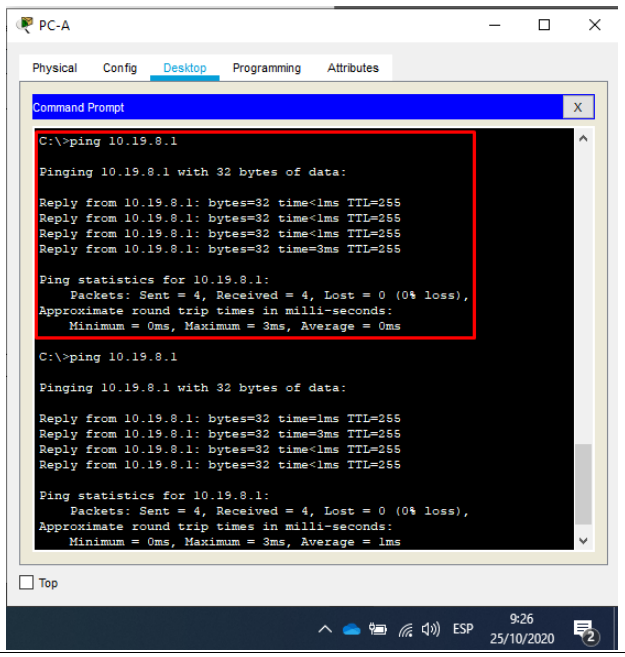
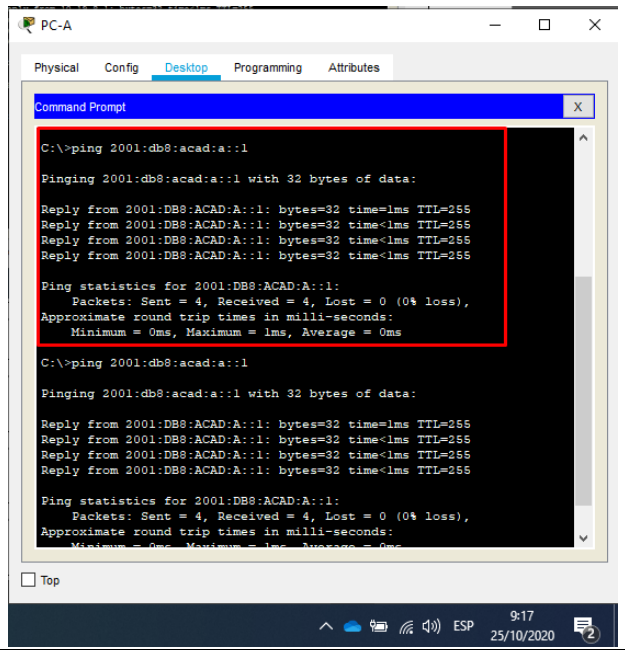
	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
	R1 Bucle 0	IPv6	2001:db8:acad:209::1	Exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
	R1 Bucle 0	IPv6	2001:db8:acad:209::1	Exitoso
	R1, G0/0/1.2	Dirección	10.19.8.1	Exitoso
	R1, G0/0/1.2	IPv6	2001:db8:acad:a::1	Exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	Exitoso
	R1, G0/0/1.3	IPv6	2001:db8:acad:b::1	Exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	Exitoso
	R1, G0/0/1.4	IPv6	2001:db8:acad:c::1	Exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Exitoso
	S2, VLAN 4	IPv6	2001:db8:acad:c::98	Exitoso
	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
	S2, VLAN 4	IPv6	2001:db8:acad:c::99	Exitoso

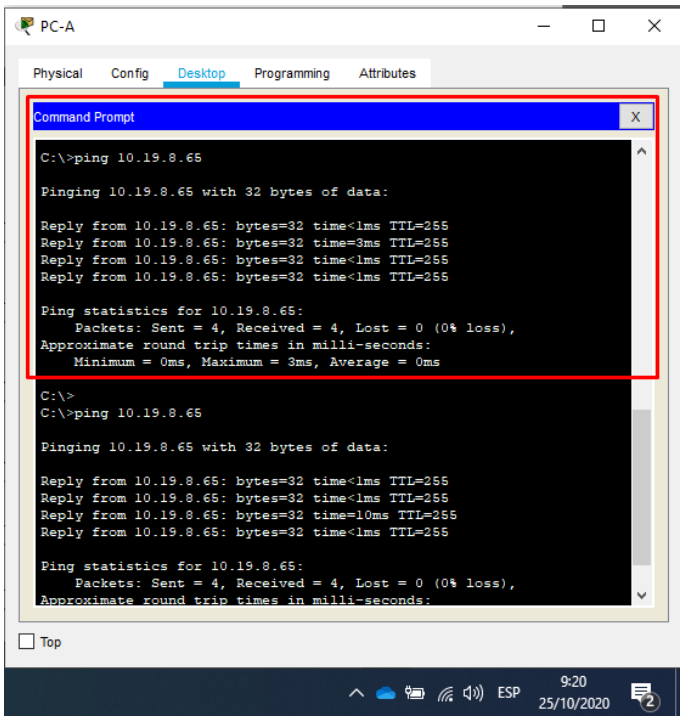
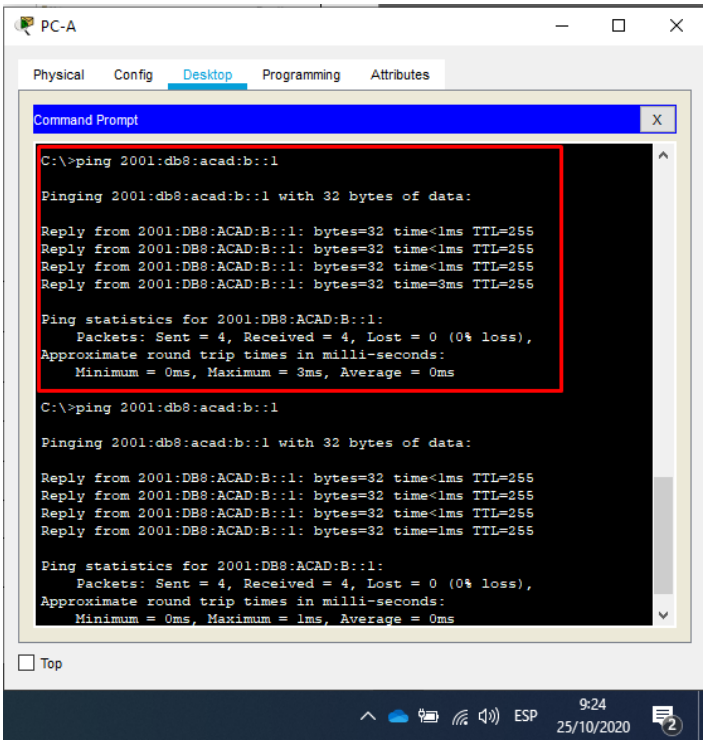
Fuente: Autor

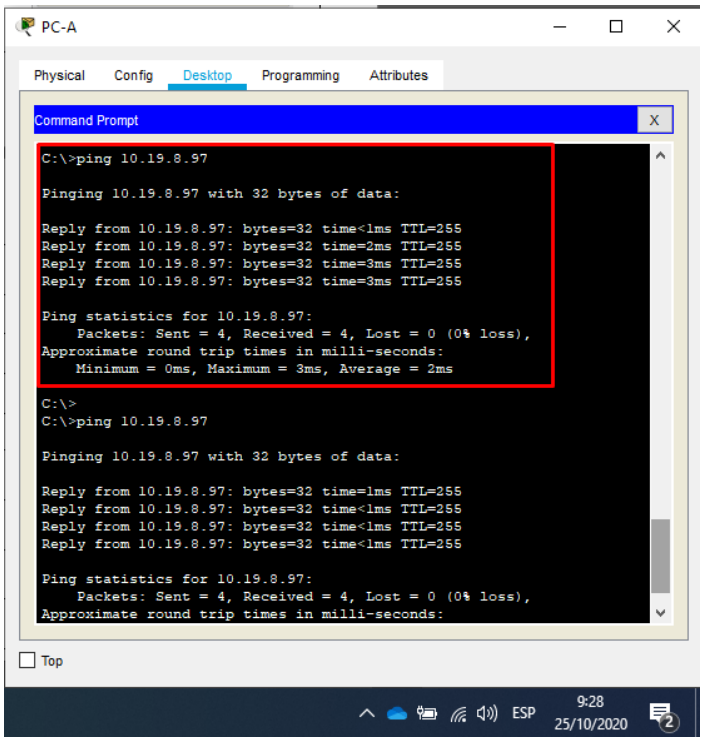
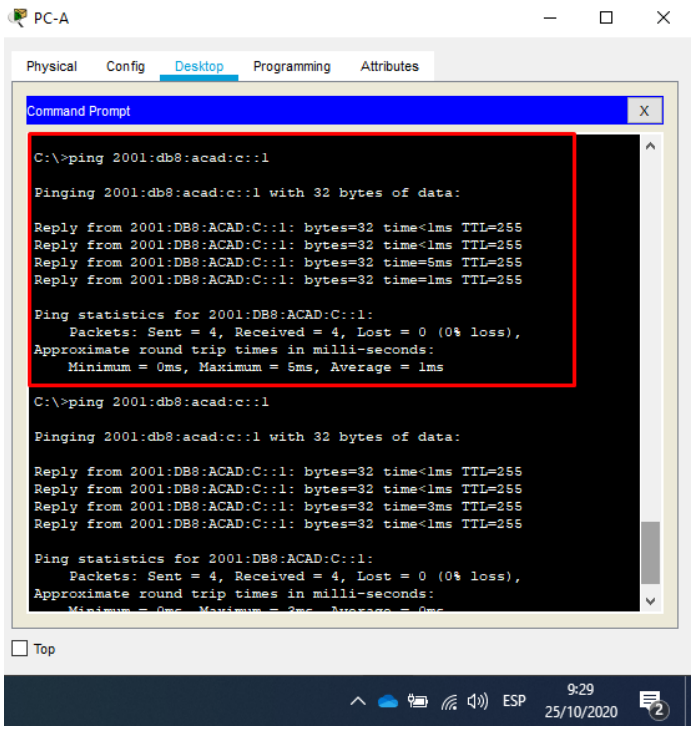
A continuación, en la Tabla 14 y Tabla 15 se realizará una a una las pruebas de conectividad ping, pruebas que ayudaran a demostrar la conectividad entre los dispositivos e interfaces de red configuradas durante la ejecución del escenario.

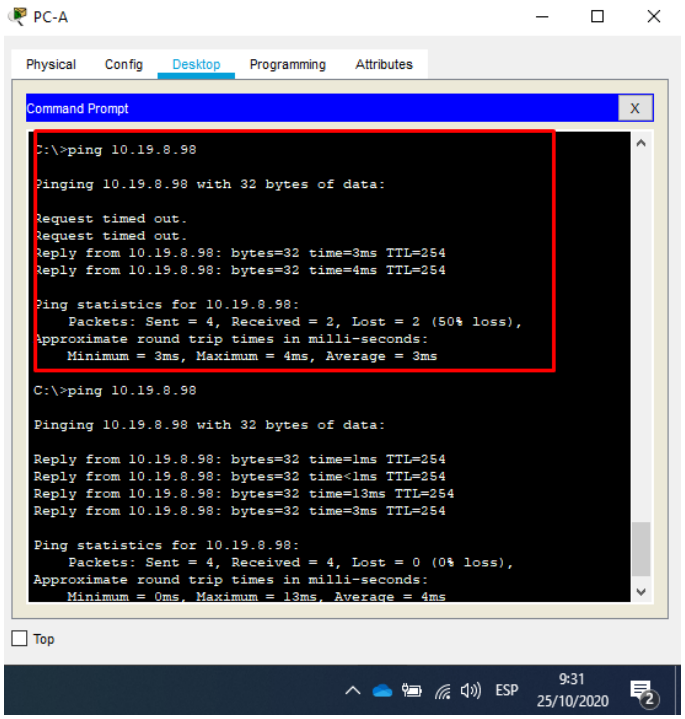
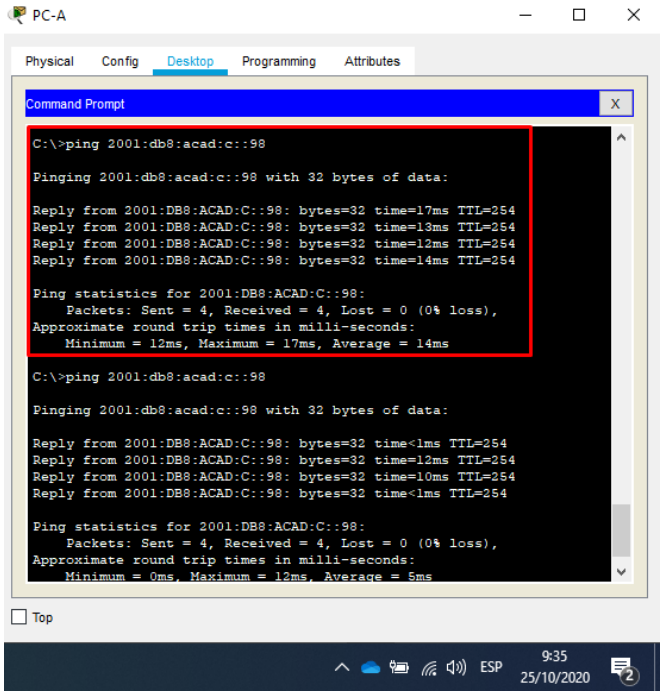
Evidencias Ping desde PC-A

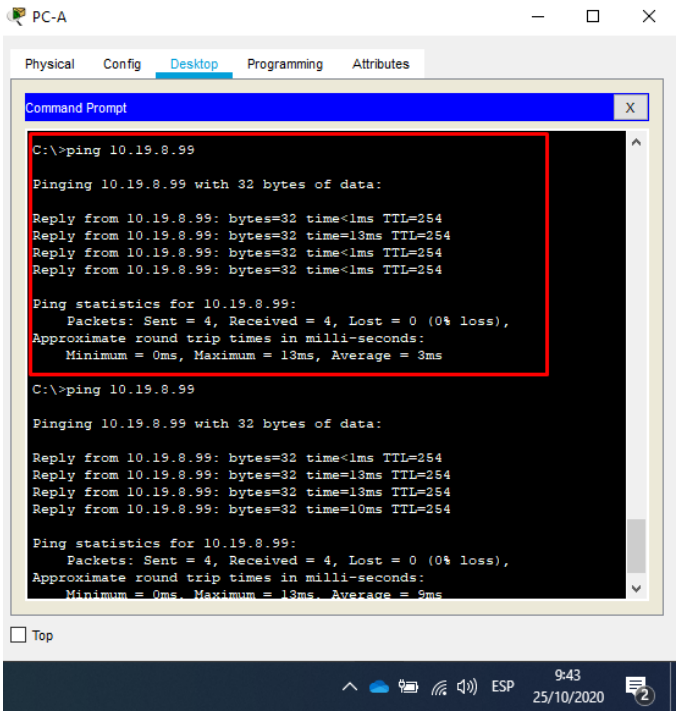
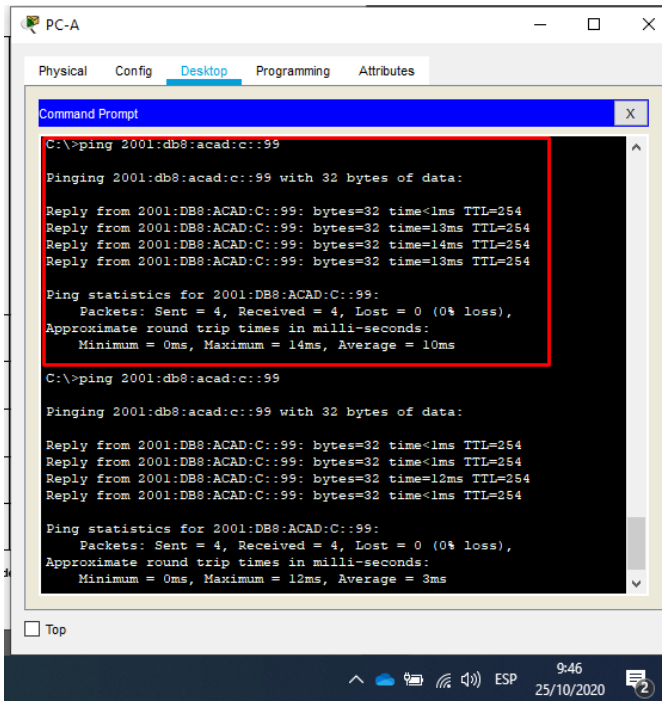
Tabla 14. Evidencias de conectividad PC-A

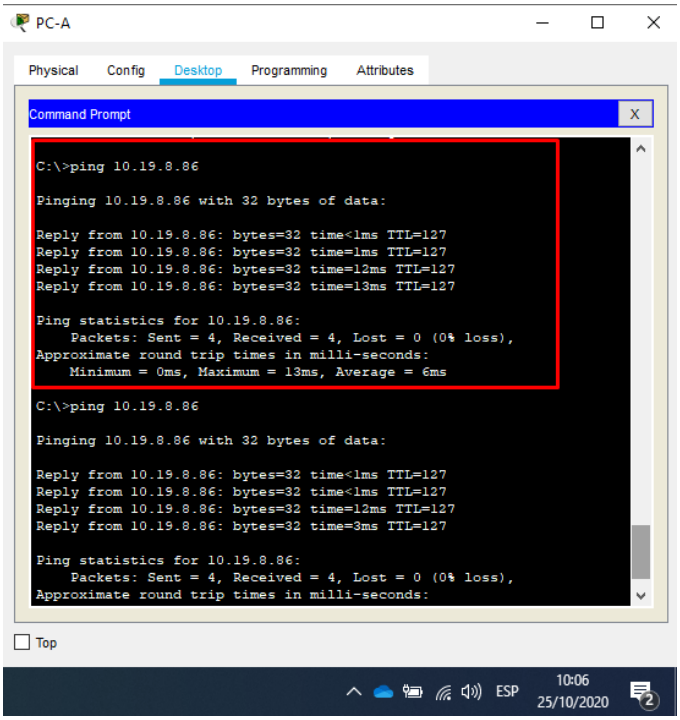
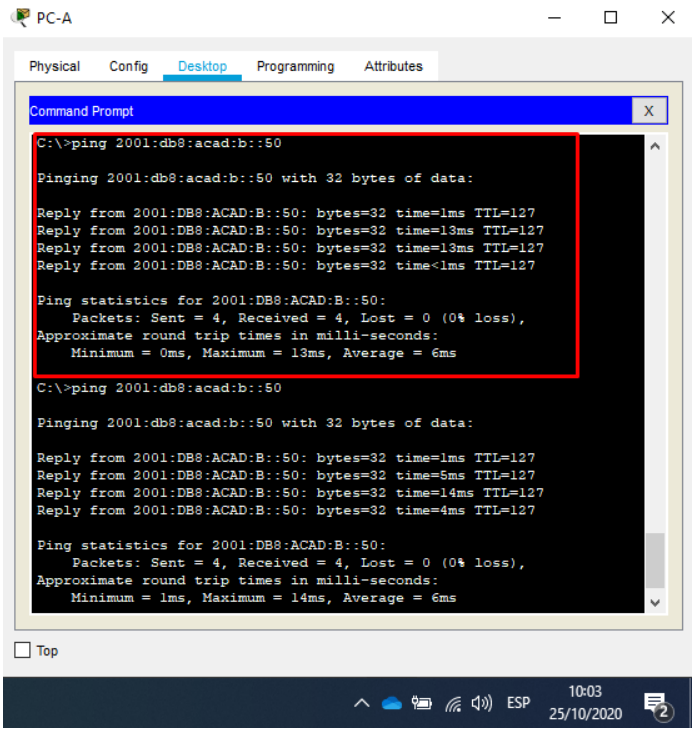
PRUEBAS DE CONECTIVIDAD PING	
Ping a la dirección 10.19.8.1	Figura 15. Ping de PC-A a IPv4 Vlan 2 R1 
Ping a la dirección 2001:db8:acad:a::1	Figura 16. Ping de PC-A a IPv6 Vlan 2 R1 

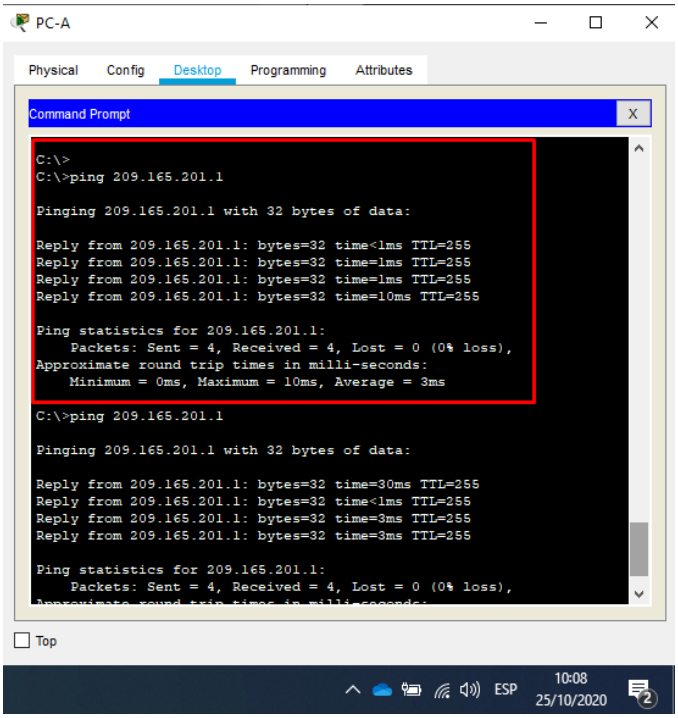
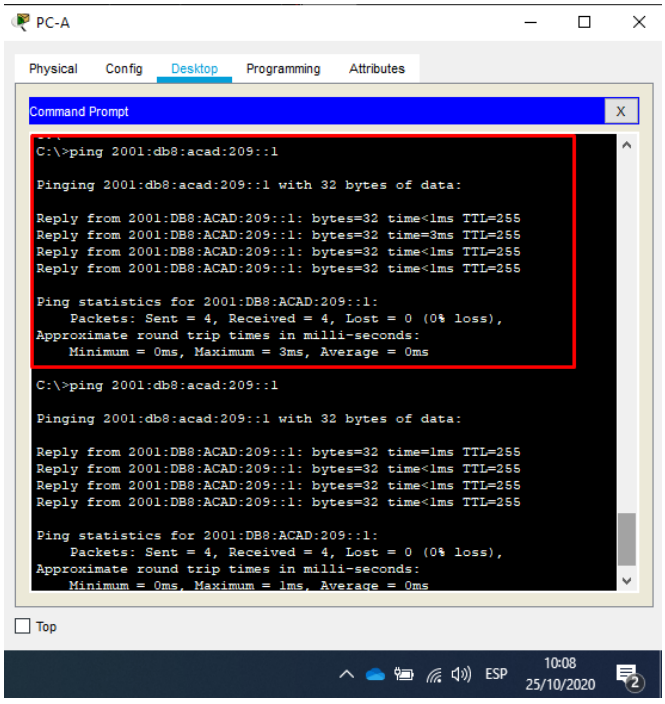
Ping a la dirección 10.19.8.65	Figura 17. Ping de PC-A a IPv4 Vlan 3 R1 
Ping a la dirección 2001:db8:acad:b::1	Figura 18. Ping de PC-A a IPv6 Vlan 3 R1 

Ping a la dirección 10.19.8.97	Figura 19. Ping de PC-A a IPv4 Vlan 4 R1 
Ping a la dirección 2001:db8:acad:c::1	Figura 20. Ping de PC-A a IPv4 Vlan 4 R1 

Ping a la dirección 10.19.8.98	Figura 21. Ping de PC-A a IPv4 Vlan 4 S1 
Ping a la dirección 2001:db8:acad:c::98	Figura 22. Ping de PC-A a IPv6 Vlan 4 S1 

Ping a la dirección 10.19.8.99	Figura 23. Ping de PC-A a IPv4 Vlan 4 S2 
Ping a la dirección 2001:db8:acad:c::99	Figura 24. Ping de PC-A a IPv4 Vlan 4 S2 

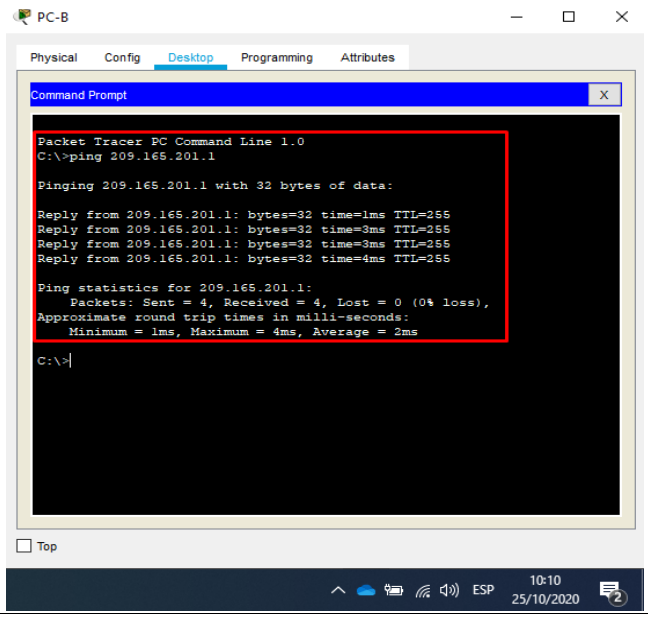
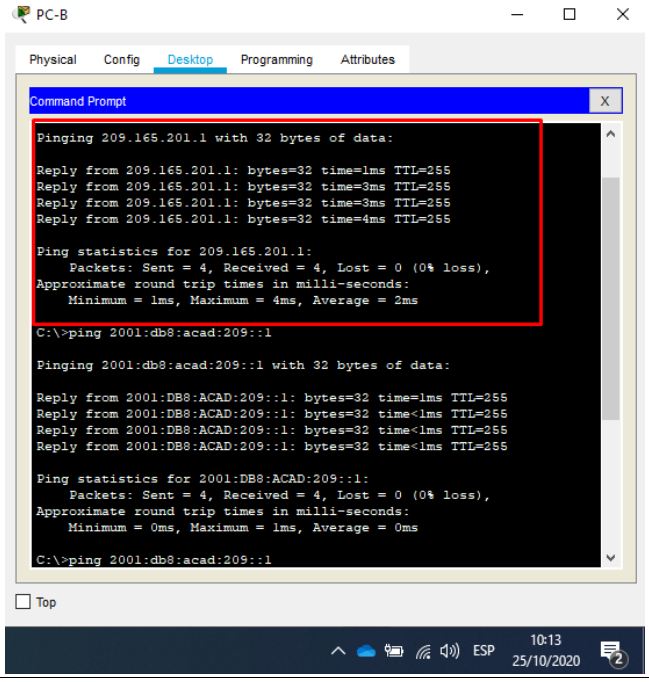
Ping a la dirección 10.19.8.86	Figura 25. Ping PC-A a PC-B para IPv4 
Ping a la dirección 2001:db8:acad:b::50	Figura 26. Ping PC-A a PC-B para IPv6 

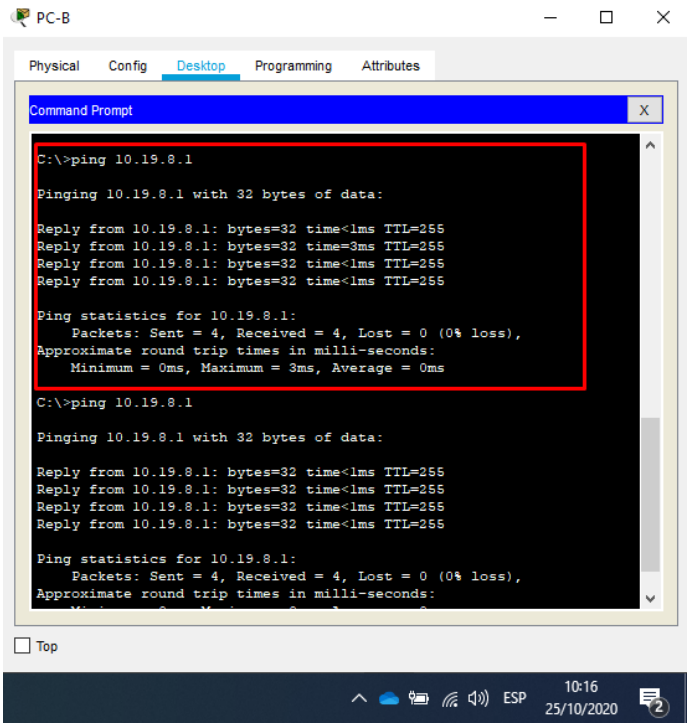
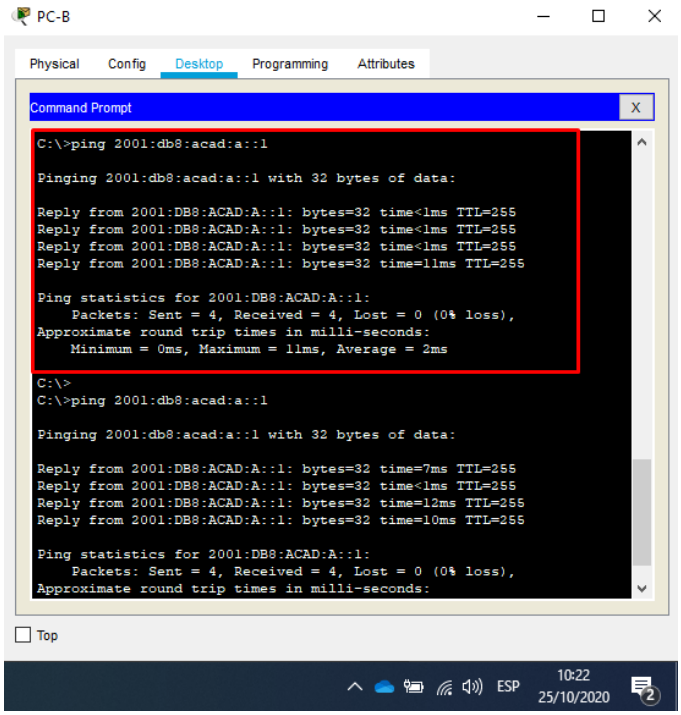
Ping a la dirección 209.165.201.1	Figura 27. Ping PC-A a Loopback0 IPv4 
Ping a la dirección 2001:db8:acad:209::1	Figura 28. Ping PC-A a Loopback0 IPv6 

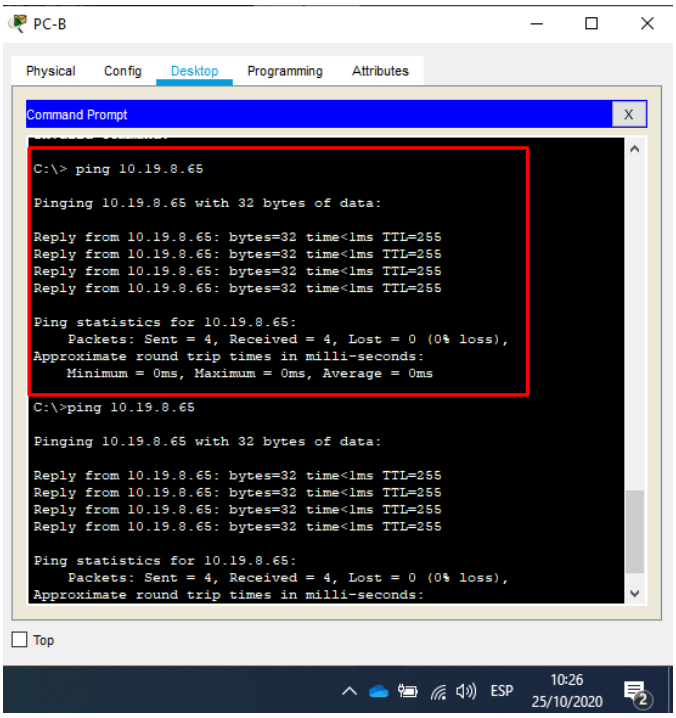
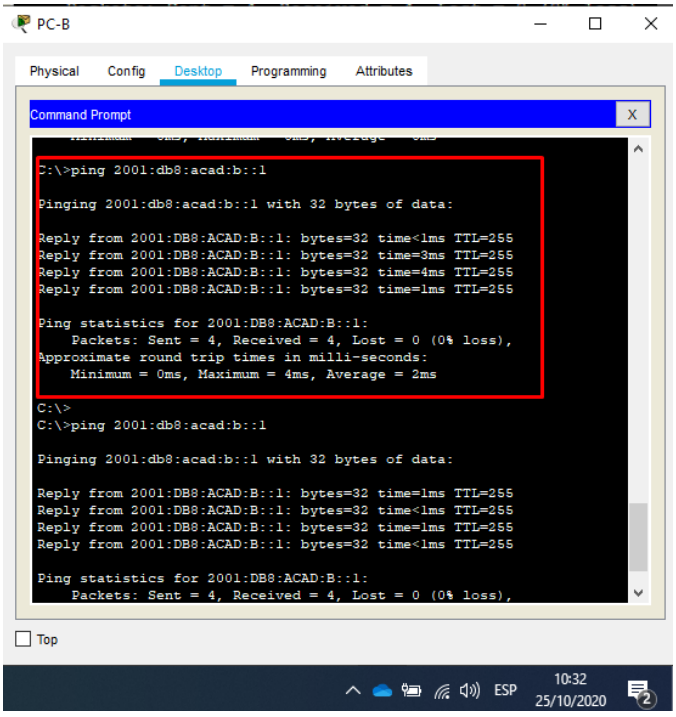
Fuente: Autor

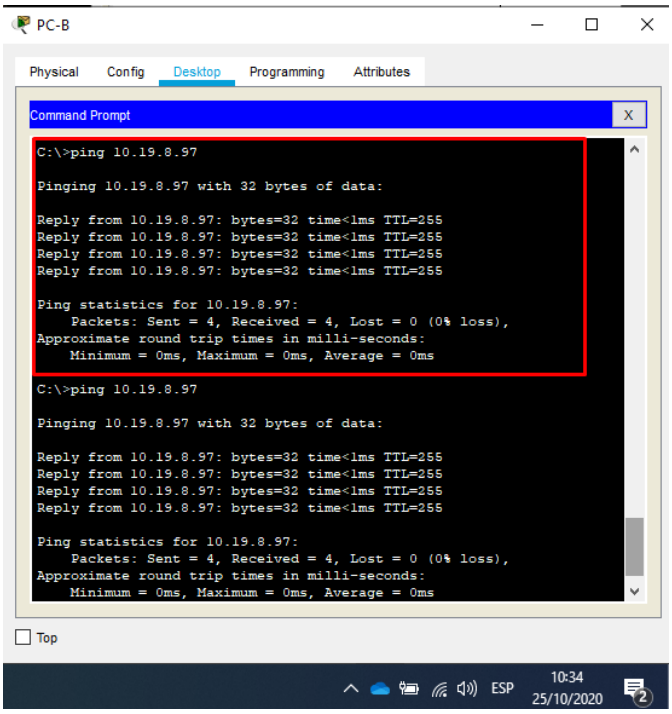
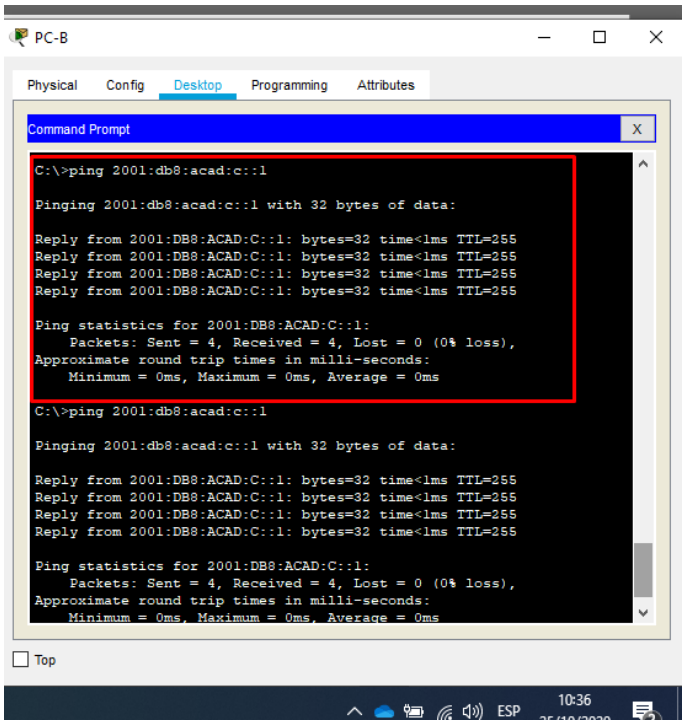
Evidencias Ping desde PC-B

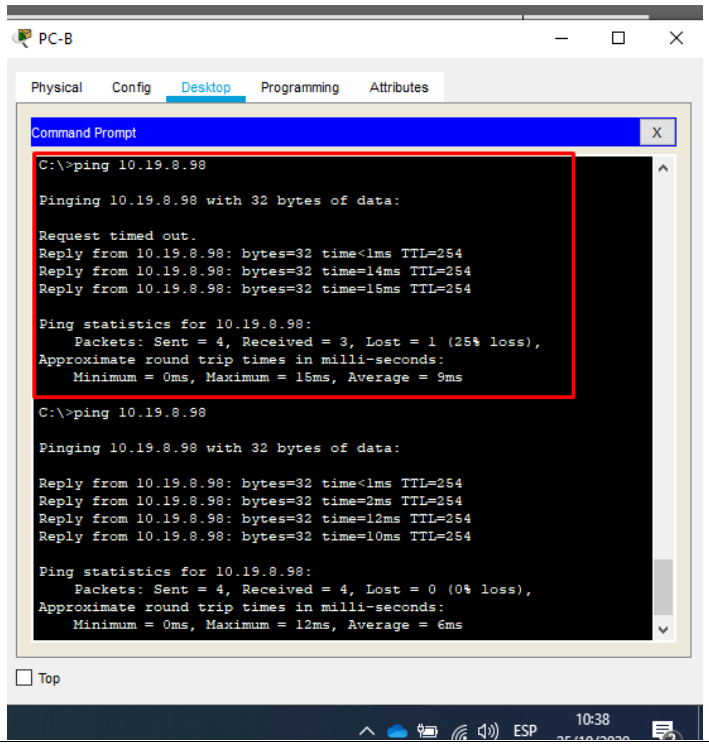
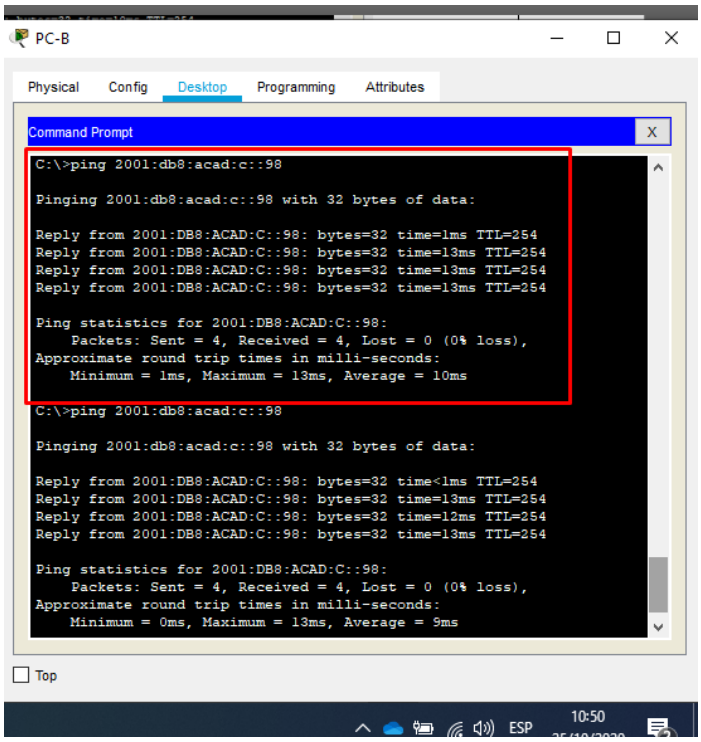
Tabla 15. Pruebas de conectividad con PC-B

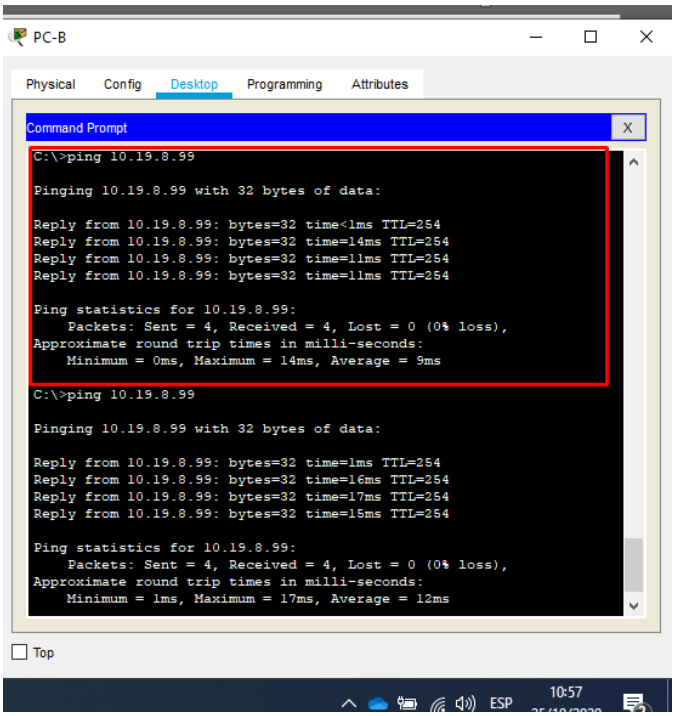
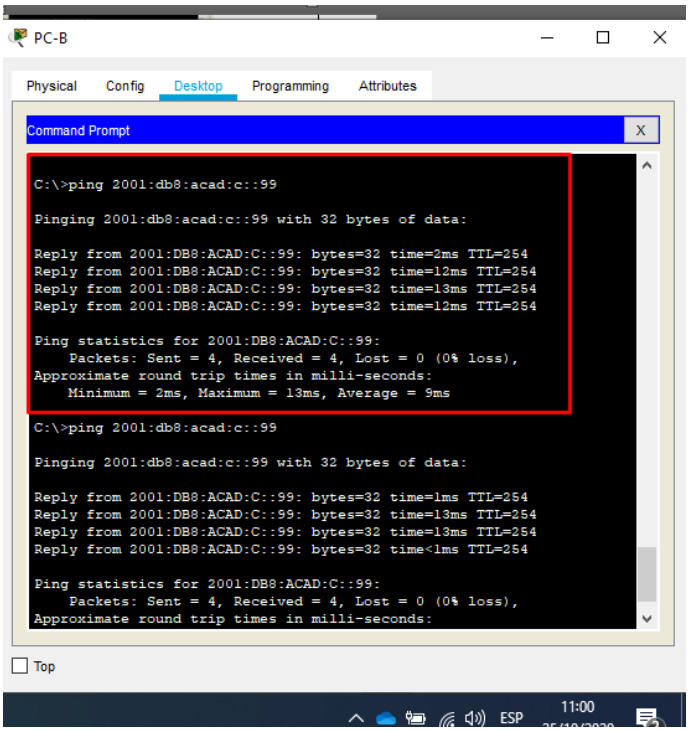
PRUEBAS DE CONECTIVIDAD PING	
Ping a la dirección 209.165.201.1	Figura 29. Ping PC-B a Loopback0 IPv4 
Ping a la dirección 2001:db8:acad:209::1	Figura 30. Ping PC-B a Loopback0 IPv6 

Ping a la dirección 10.19.8.1	Figura 31. Ping de PC-B a IPv4 Vlan 2 R1 
Ping a la dirección 2001:db8:acad:a::1	Figura 32. Ping de PC-B a IPv6 Vlan 2 R1 

Ping a la dirección 10.19.8.65	Figura 33. Ping de PC-B a IPv4 Vlan 3 R1 
Ping a la dirección 2001:db8:acad:b::1	Figura 34. Ping de PC-B a IPv6 Vlan 3 R1 

Ping a la dirección 10.19.8.97	Figura 35. Ping de PC-B a IPv4 Vlan 4 R1 
Ping a la dirección 2001:db8:acad:c::1	Figura 36. Ping de PC-B a IPv6 Vlan 4 R1 

Ping a la dirección 10.19.8.98	Figura 37. Ping de PC-B a IPv4 Vlan 4 S1 
Ping a la dirección 2001:db8:acad:c::98	Figura 38. Ping de PC-B a IPv6 Vlan 4 S1 

Ping a la dirección 10.19.8.99	Figura 39. Ping de PC-B a IPv4 Vlan 4 S2 
Ping a la dirección 2001:db8:acad:c::99	Figura 40. Ping de PC-B a IPv4 Vlan 4 S2 

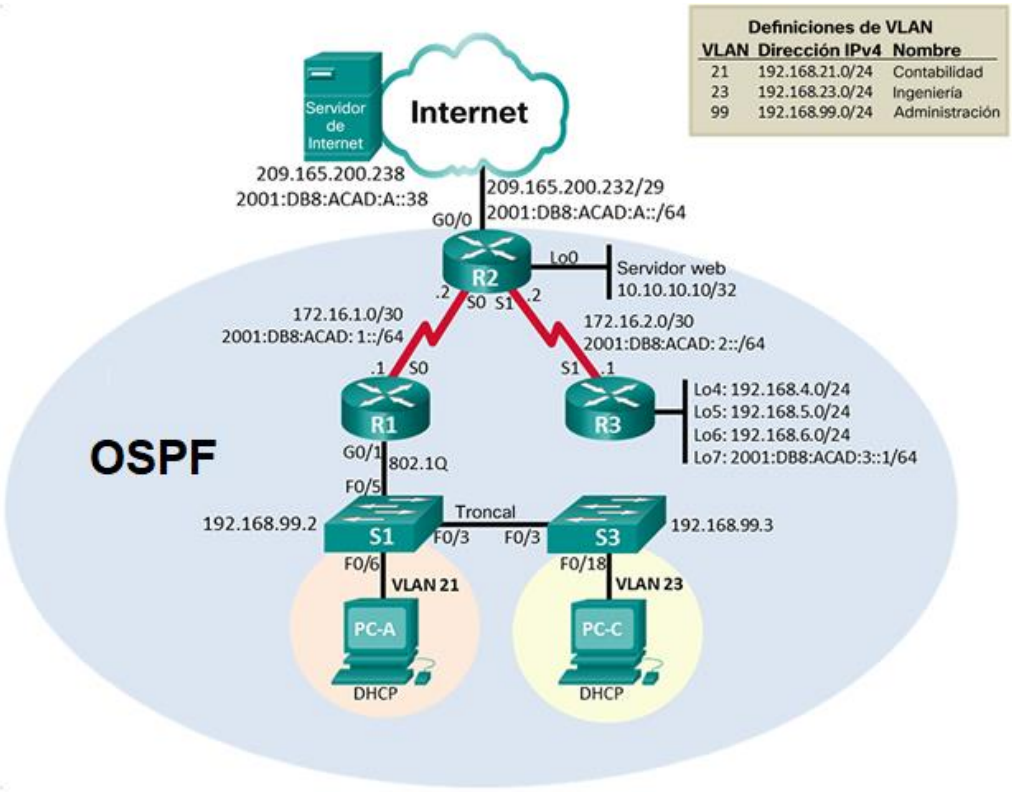
Fuente: Autor

Al haber ejecutado todas las pruebas ping listadas en las tablas anteriores, se pudo verificar la conectividad entre todos los dispositivos e interfaces virtuales de red, por lo que se demuestra la conexión mediante los direccionamientos configurados bajo Ipv4 e Ipv6.

1.2. ESCENARIO 2

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 41. Topología escenario 2



Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

A continuación, en la Tabla 16 se listarán cada uno de los comandos necesarios para eliminar las configuraciones de fabrica presentes en los router y switches.

Tabla 16. Reinicio y recarga de router

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash:

Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

A continuación, en la Tabla 17 se muestran los parámetros IP que deben se configurados en el servidor Web:

Tabla 17. Parámetros de configuración de servidor Web

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

Fuente: Autor

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Parámetros de configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router: R1	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada: class	R1(config)#enable password class
Contraseña de acceso a la consola: cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet: cisco	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
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 prohíbe el acceso no autorizado.#
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config)#int serial 0/0/0 R1(config-if)#description conexión a 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 shutdown

Rutas predeterminadas Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::00/0 s0/0/0

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 1 cuente con seguridad, ya que en adelante solicitara contraseña para el acceso a través de consola al igual que para el acceso remoto a través de las líneas VTY. Por otra parte, se configuro el direccionamiento IP para la interfaz serial, también crearon las rutas estáticas por defecto, para que, de no encontrarse la red solicitada en la tabla de enrutamiento, esta no sea descartada, si no que salga por la interfaz s0/0/0 en busca de la red de destino mediante el otro router.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Parámetros de configuración 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 password class
Contraseña de acceso a la consola: cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet: cisco	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption

Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD: Se prohíbe el acceso no autorizado.	R2(config)# banner motd # Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2(config)#int serial 0/0/0 R2(config-if)#description conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2(config)#interface serial 0/0/1 R2(config-if)#description conexion a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet) Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config)#interface gigabitEthernet 0/0 R2(config-if)#description Conexión hacia Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado) Establecer la descripción.	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255

Establezca la dirección IPv4.	R2(config-if)#description Servidor Web R2(config-if)#exit
Ruta predeterminada Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R2(config)#ipv6 route ::00/0 s0/0/0

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 2 cuente con seguridad, ya que en adelante solicitara contraseña para el acceso a través de consola al igual que para el acceso remoto a través de las líneas VTY. Por otra parte, se configuro el direccionamiento IP para las interfaces seriales y Ethernet, también crearon las rutas estáticas por defecto, para que, de no encontrarse la red solicitada en la tabla de enrutamiento, esta no sea descartada, si no que salga por la interfaz s0/0/0 en busca de la red de destino mediante el otro router. Finalmente se configuro la interfaz loopback 0 para simular en servidor web al que se le habilitaron los correspondientes servicios mediante el comando indicado.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Parámetros de configuración 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 password class
Contraseña de acceso a la consola: cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet: cisco	R3(config)#line vty 0 15 R3(config-line)#password cisco

	R3(config-line)#login R3(config-line)#exit
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 prohíbe el acceso no autorizado.#
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3(config)#interface serial 0/0/1 R3(config-if)#description Conexión a R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7 Establezca la dirección IPv6. Consulte el diagrama de	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

topología para conocer la información de direcciones.	R3(config-if)#exit
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R2(config)#ipv6 route ::00/0 s0/0/1

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 3 cuente con seguridad, ya que en adelante solicitara contraseña para el acceso a través de consola al igual que para el acceso remoto a través de las líneas VTY. Por otra parte, se crearon las interfaces loopback 4,5,6 y 7 a las que se les configuro el direccionamiento IP correspondiente, también se configuro el direccionamiento y propiedades de la interfaz serial, Finalmente, se crearon las rutas estáticas por defecto, para que, de no encontrarse la red solicitada en la tabla de enrutamiento, esta no sea descartada, si no que salga por la interfaz s0/0/1 en busca de la red de destino mediante el otro router

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 21. Parámetros de configuración S1 escenario 2

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 password class
Contraseña de acceso a la consola: cisco	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet: cisco	S1(config)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encription

Mensaje MOTD: Se prohíbe el acceso no autorizado.	S1(config)#banner motd #Se prohíbe el acceso no autorizado. #

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que los switch 1 cuente con su nombre asignado para la práctica, se desactive la búsqueda de comandos erróneos a través de DNS, también que tenga los parámetros básicos seguridad, en adelante solicitara contraseña para el acceso a través de puerto de consola y telnet mediante las líneas vty. Por otra parte, se emitirá siempre un mensaje antes del acceso a fin de informar la propiedad y administración del dispositivo.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 22. Parámetros de configuración S3 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch: S3	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada: class	S3(config)#enable password class
Contraseña de acceso a la consola: cisco	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet: cisco	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encription
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado. #

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que los switch 3 cuente con su nombre asignado para la práctica, se desactive la búsqueda de comandos erróneos a través de DNS, también que tenga los parámetros básicos seguridad, en adelante solicitara contraseña para el acceso a través de puerto de consola y telnet mediante las líneas vty. Por otra parte, se emitirá siempre un mensaje antes del acceso a fin de informar la propiedad y administración del dispositivo.

Paso 7: Verificar la conectividad de la red

A continuación, en la Tabla 23 se muestran las pruebas de conectividad ping que se realizaran, con el fin de probar la conectividad en los router y pc de Internet:

Tabla 23. Pruebas de conectividad Ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2/30 2001:DB8:ACAD:1::2	Exitoso
R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

Tabla 24. Evidencias de conectividad entre Reuters

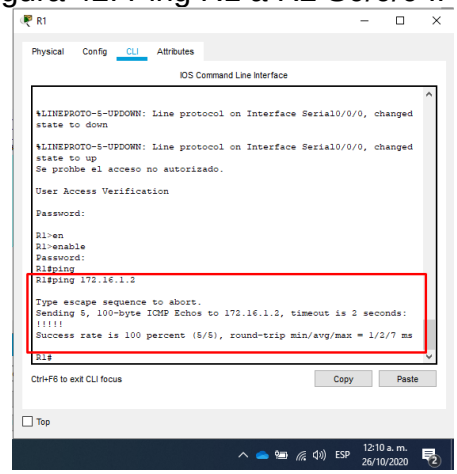
EVIDENCIAS DE PING ENTRE REUTERS	
Pruebas de conectividad Ping: R1 a R2 S0/0/0: Ipv4:172.16.1.2 Ipv6:2001:DB8:ACAD:1::2	Figura 42. Ping R1 a R2 S0/0/0 IPv4 

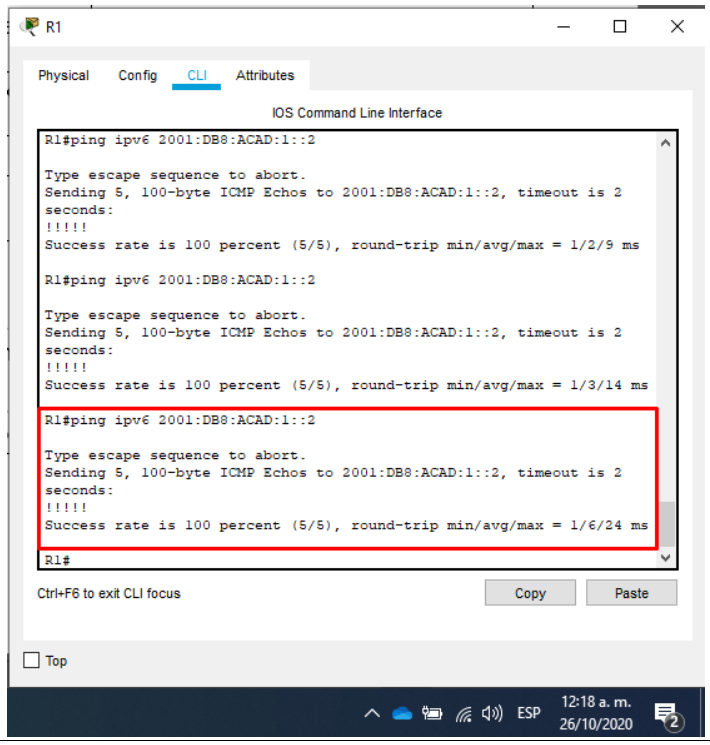
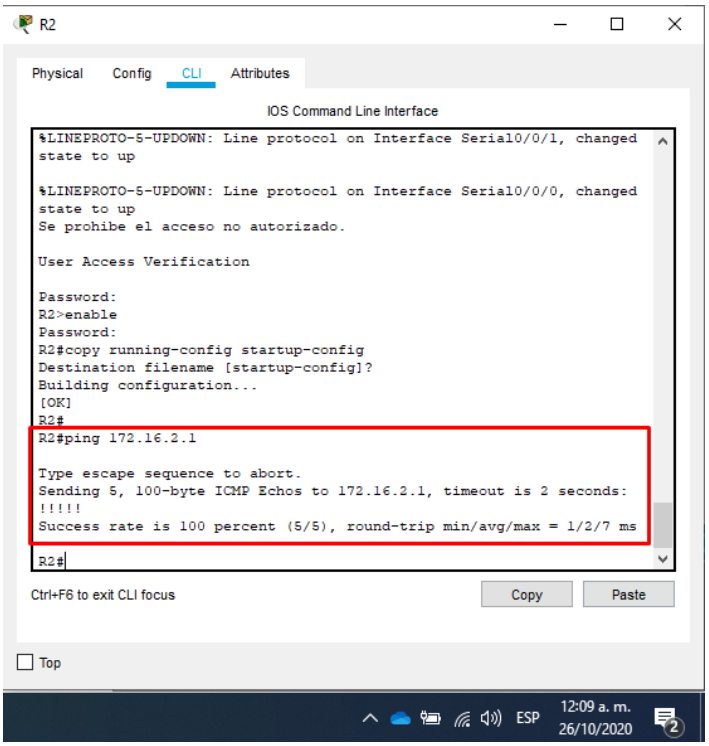
	Figura 43. Ping R1 a R2 S0/0/0 IPv6 
Pruebas de conectividad Ping: R2 a R3 S0/0/1: Ipv4:172.16.2.1 Ipv6:2001:DB8:ACAD:2::1	Figura 44. Ping R2 a R3 S0/0/1 IPv4 

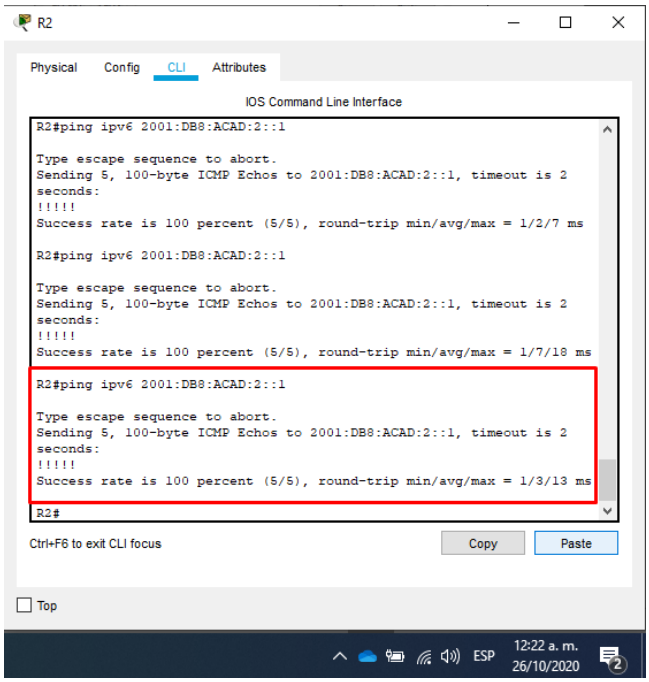
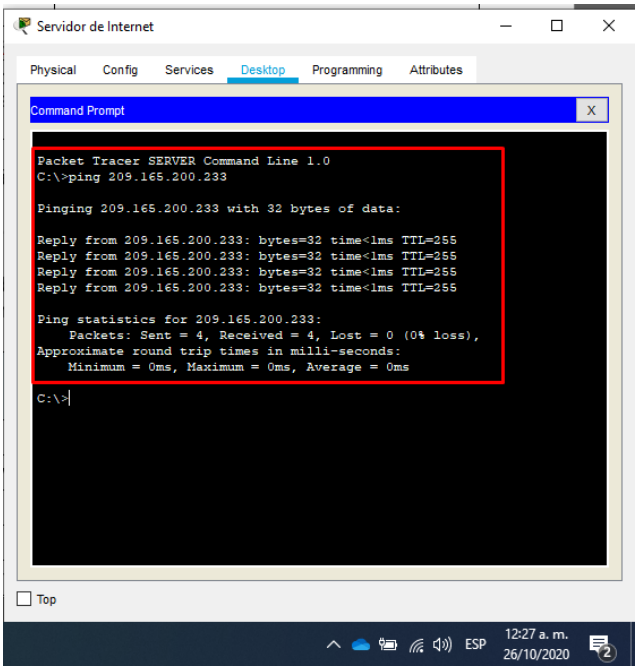
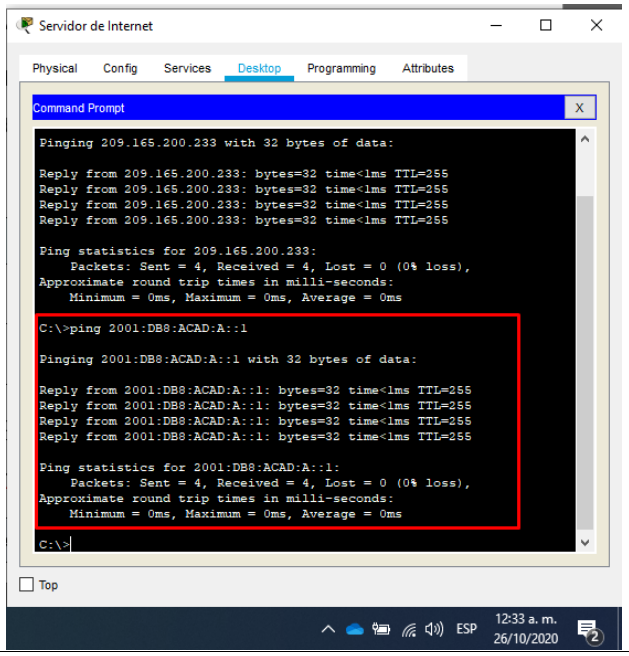
	Figura 45. Ping R2 a R3 S0/0/1 IPv6 
Pruebas de conectividad Ping: PC de Internet a Puerta de enlace predeterminada 209.165.200.233 2001:DB8:ACAD:A::1	Figura 46. Ping PC de Internet a Puerta de enlace predeterminada IPv4 

	Figura 47. Ping PC de Internet a Puerta de enlace predeterminada IPv4 

Fuente: Autor

Al haber ejecutado todas las pruebas ping listadas en la tabla anterior, se pudo verificar la conectividad entre los routers y servidor Web, por lo que se demuestra la conexión mediante los direccionamientos configurados bajo Ipv4 e Ipv6.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 25. Configuración de parámetros Vlan en S1 escenario 2

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	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23

cada una de las VLAN que se indican	S1(config-vlan)#name Ingeniería S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administración
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0
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 mode trunk S1(config-if)#switchport trunk native vlan 99 S1(config-if)#no shutdown
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 mode trunk S1(config-if)#switchport trunk native vlan 99 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso: Utilizar el comando interface range	S1(config)#interface range f0/1-2,f0/4,f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2,f0/4,f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que los switch 1 cuente con puerta de enlace predeterminada, que sean creadas las Vlan 21,23 y 99 necesarias para el escenario, también se configuro la 99 como interfaz de gestión, se configuraron las interfaces troncales en los puertos Fe0/3 y Fe0/5, se asignó la Vlan 21 al puerto Fe0/6 y el resto de puertos fueron configurados en modo acceso y desactivados administrativamente por seguridad.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 26. Configuración de parámetros Vlan en S3 escenario 2

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)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingeniería S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administración S3(config-vlan)#exit
Asignar la dirección IP de administración: Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	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)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso utilizando el comando interface range	S3(config)# interface range f0/1-2,f0/4-24, g0/1-2S1(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S1(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)# interface range f0/1-2,f0/4-17,f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que los switch 3 cuente con puerta de enlace predeterminada, que sean creadas las Vlan 21,23 y 99 necesarias para el escenario, también se configuro la 99 como interfaz de gestión, se configuraron la interfaz troncal en la Fe0/3, se asignó la Vlan 23 al puerto Fe0/ y el resto de puertos fueron configurados en modo acceso y desactivados administrativamente por seguridad.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 27. Parámetros de configuración subinterfaces R1 escenario 2

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 Interface Gtw Vlan 21 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 gigabitEthernet 0/1.23 R1(config-subif)#description Interface Gtw Vlan 23 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 gigabitEthernet 0/1.99 R1(config-subif)#description Interface Gtw Vlan 99 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 gigabitEthernet 0/1 R1(config-if)#no shutdown

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 1 cuente con dos subinterfaces creadas y configuradas con sus respectivas Ip, cuyo propósito es brindar enrutamiento a las dos redes que están asignadas mediante las Vlan 21 y 23 que van encapsuladas por la interface Ge0/1 del router haca sus destinos.

Paso 4: Verificar la conectividad de la red

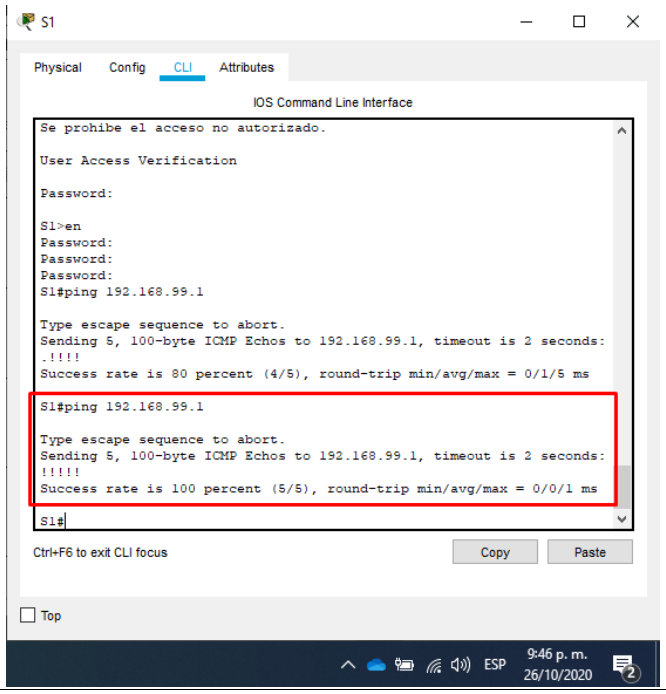
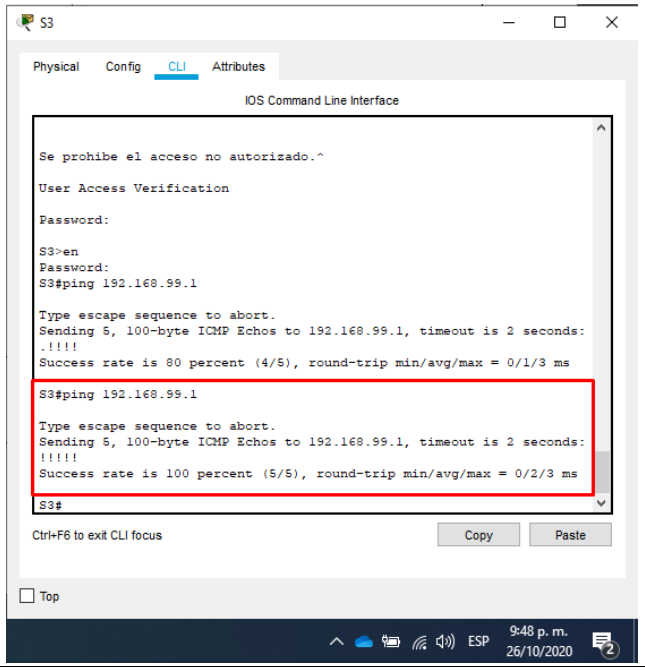
Utilice el comando ping para probar la conectividad entre los switches y el R1.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

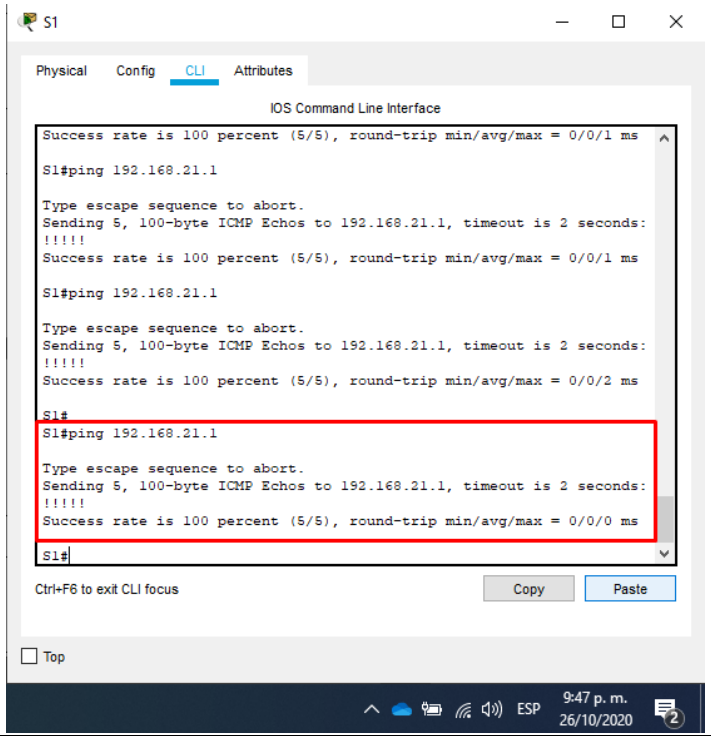
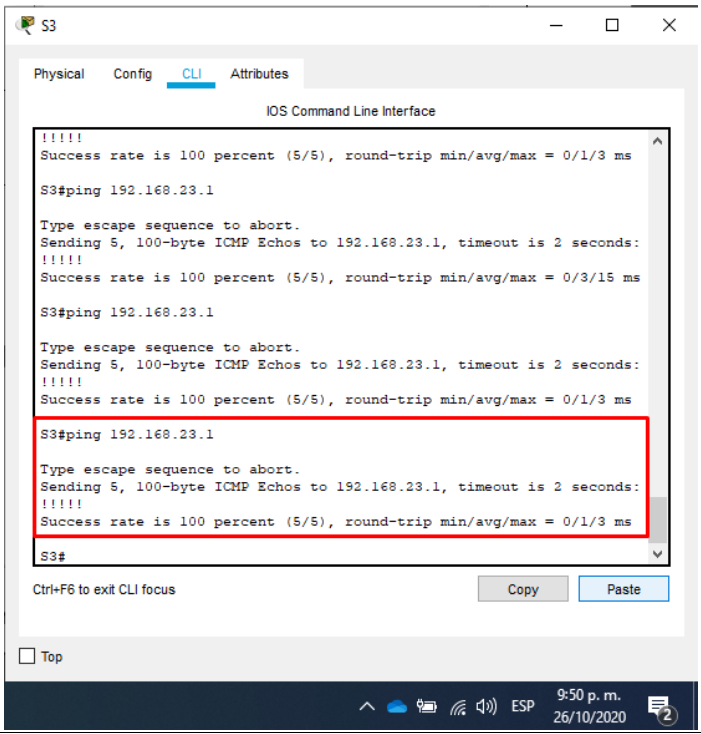
Tabla 28. Pruebas de conectividad Ping entre switches y R1

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

Fuente: Autor

Tabla 29. Evidencias de conectividad de switches

<table>
<tr><th colspan="2">Evidencias de conectividad de switches</th></tr>
<tr><td>Pruebas de conectividad Ping: S1 a R1, dirección VLAN 99
Ipv4:192.168.99.1</td><td>Figura 48. Ping S1 a R1, dirección VLAN 99
 
</td></tr>
<tr><td>Pruebas de conectividad Ping: S3 a R1, dirección VLAN 99
Ipv4:192.168.99.1</td><td>Figura 49. Ping S3 a R1, dirección VLAN 99
 
</td></tr>
</table>

Pruebas de conectividad Ping: S1 a R1, dirección VLAN21 Ipv4:192.168.21.1	Figura 50. Ping S1 a R1, dirección VLAN21 
Pruebas de conectividad Ping: S3 a R1, dirección VLAN23 Ipv4:192.168.23.1	Figura 51. Ping S3 a R1, dirección VLAN23 

Fuente: Autor

Al haber ejecutado todas las pruebas ping listadas en la tabla anterior, se pudo verificar la conectividad entre los routers y switches de la red, por lo que se demuestra el poder realizar gestión a los dispositivos mediante los direccionamientos configurados bajo Ipv4 para las Vlan 21,23 y 99.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 30. Parámetros de configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	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 g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)# no auto-summary

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra activar en el router 1 el enrutamiento dinámico OSPF con el área 0, también se agregaron las redes conectadas directamente al router, con el fin de que fuesen asociadas al área 0 del OSPF, y como condición adicional se desactivo la sumarización de redes.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 31. Parámetros de configuración OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1
Anunciar las redes conectadas directamente **Nota:** Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0.0.255 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)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)# auto-summary

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra activar en el router 2 el enrutamiento dinámico OSPF con el área 0, también se agregaron las redes conectadas directamente al router, con el fin de que fuesen asociadas al área 0 del OSPF, como condición adicional se configuro la interfaz pasiva la loopback 0 para evitar el envío de mensajes routing por esta interfaz y se desactivo la sumarización de redes.

Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 32. Parámetros de configuración OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1
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
Desactive la sumarización automática.	R3(config-router)# auto-summary

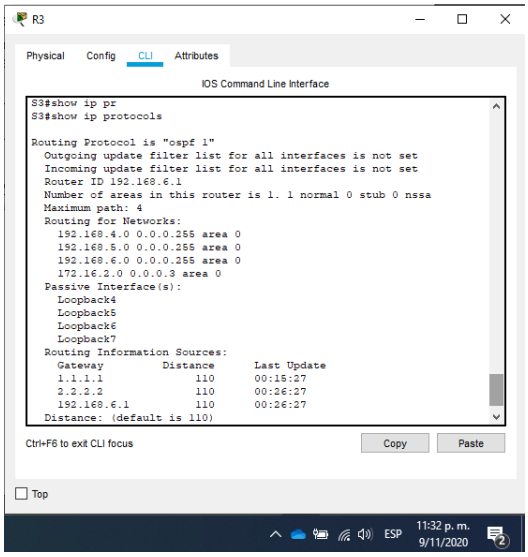
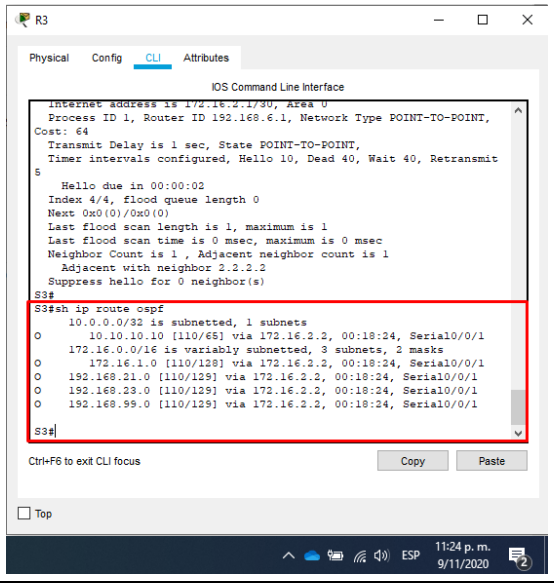
Fuente: Autor

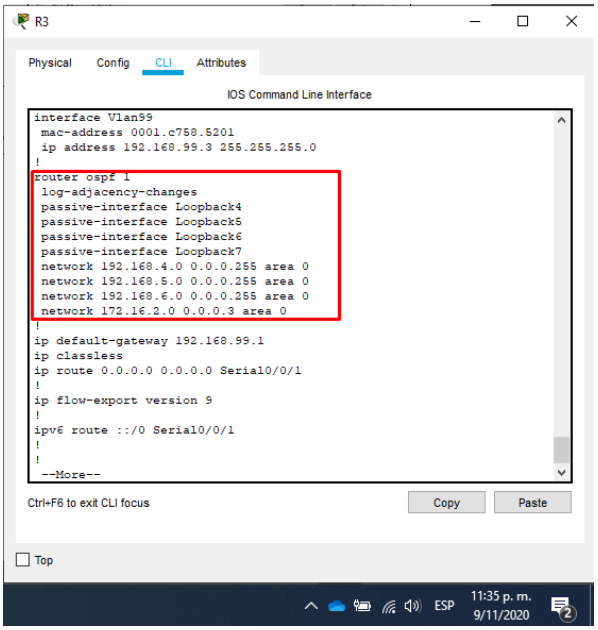
Al haber aplicado los comandos anteriores, se logra activar en el router 3 el enrutamiento dinámico OSPF con el área 0, también se agregaron las redes conectadas directamente al router, con el fin de que fuesen asociadas al área 0 del OSPF, como condición adicional se configuro las interfaces pasivas las loopback 4,5,6 y 7 para evitar el envío de mensajes routing mediante estas interfaces y se desactivo la sumarización de redes.

Paso 4: Verificar la información de OSPF

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

Tabla 33. Verificación de parámetros OSPF en routers

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? **Rta:** Con el comando Show **ip protocols**	Figura 52. Ejecución comando Show ip protocols 
¿Qué comando muestra solo las rutas OSPF? **Rta:** Con el comando **show ip route ospf**	Figura 53. Ejecución comando show ip route ospf 

¿Qué comando muestra la sección de OSPF de la configuración en ejecución? **Rta:** Con el comando **show running-config**	Figura 54. Ejecución comando show running-config 

Fuente: Autor

Al haber ejecutado todos los comandos anteriores, se puedo verificar visualmente la configuración y estado del enrutamiento dinámico OSPF, en donde se pueden visualizar todas las redes que componen el área 0 del enrutamiento dinámico.

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 34. Parámetros de configuración DHCP en R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

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

Fuente: Autor

Al haber aplicado los comandos anteriores, se logra que el router 1 asigne dirección IP a los hosts mediante la activación del servicio de DHCP, esta configuración agrego cada pool al dominio ccna-sa.com, se excluirá un rango de 20 IP's para cada uno de los pools configurados, por otra parte, se distribuirá su respectiva puerta de enlace a cada uno de los hosts.

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

La configuración del R2 incluye las siguientes tareas:

Tabla 35. Parámetros de configuración NAT

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#username webuser privilege 15 secret cisco12345

Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**	
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http autentication local
Crear una NAT estática al servidor web. Dirección global interna: **209.165.200.237**	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 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 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.233** – **209.165.200.236**	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

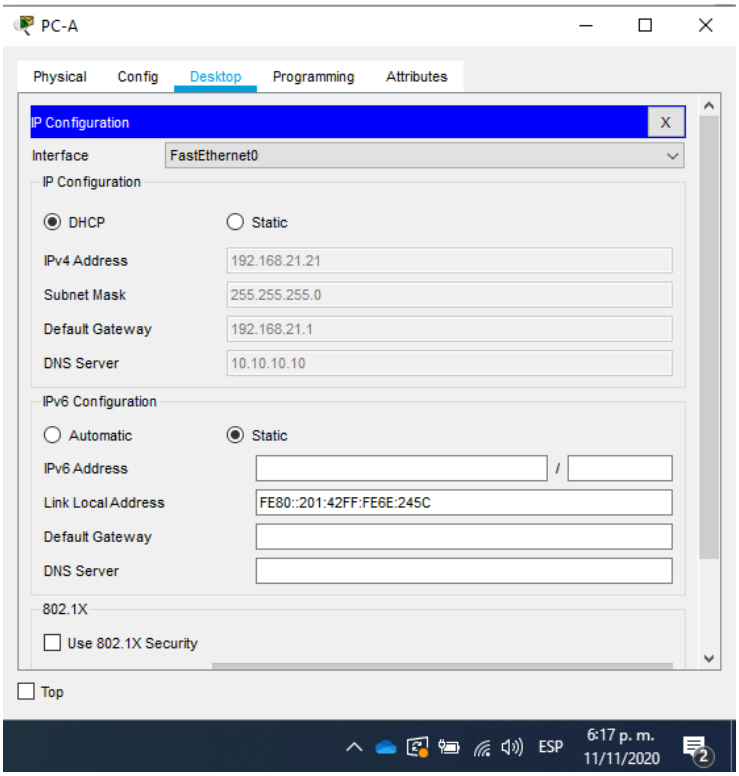
Fuente: Autor

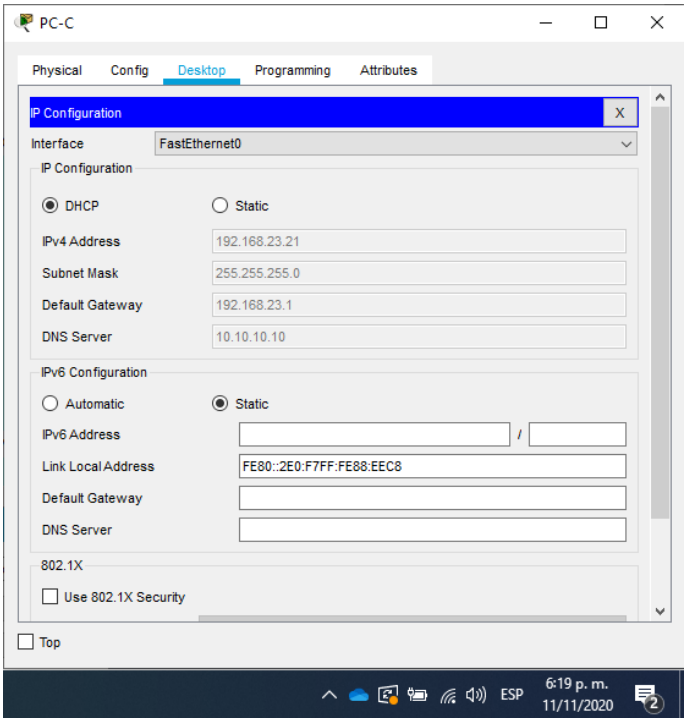
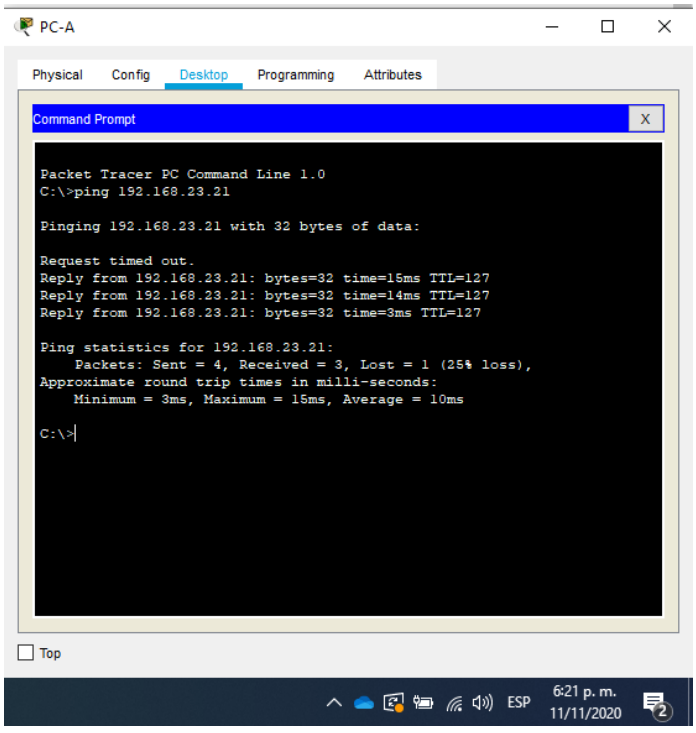
Al haber aplicado los comandos anteriores, se logra que el router 2 se active el servicio de servidor HTTP, se crea usuario y contraseña para realizar autenticación para la gestión al servicio HTTP, se configuran las interfaces internas y externas para el NAT, por otro lado, a través de una lista de acceso se permite la traducción de direcciones para conectividad a internet. Finalmente se establece el pool de direcciones mediante los cuales se traducirán para salir a Internet.

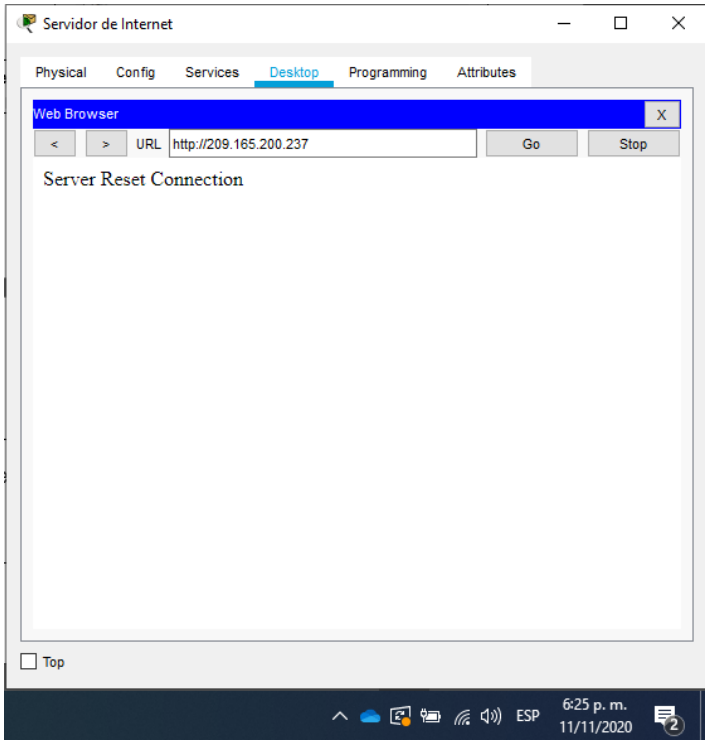
Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 36. Verificación de funcionamiento protocolos DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 55. Verificación de asignación de DHCP PC-A 

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 56. Verificación de asignación de DHCP PC-C 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 57. Verificación de conectividad con PC-C 

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Figura 58. Simulación de ingreso a servidor Web 

Fuente: Autor

Al haber ejecutado todos los comandos anteriores, se puedo verificar visualmente como el servicio de DHCP configurado en el router 1 es entregado a los host PC-A y PC-C, por otro lado, se verifico la conectividad ping entre los dos dispositivos, al igual que la verificación del acceso al servicio HTTP con sus respectivas credenciales de seguridad.

Parte 6: Configurar NTP

Tabla 37. Parámetros de configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. **5 de marzo de 2016, 9 a. m.**	R2(config)#clock set 09:00:00 5 march 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.	R1(config)#show ntp associations

Fuente: Autor

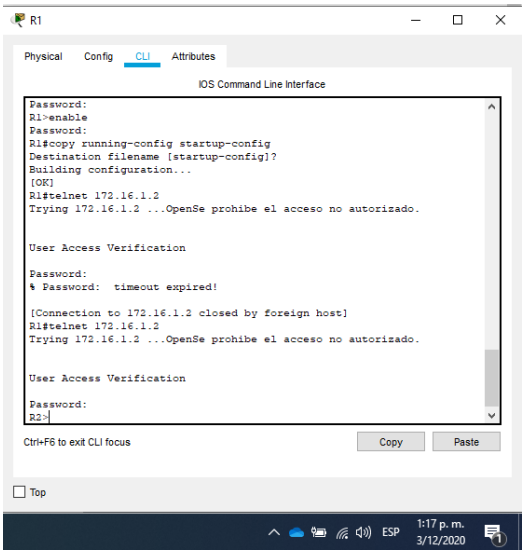
Al haber ejecutado todos los comandos anteriores, se estableció la hora de forma manual al router 2, por otra parte, este fue establecido como servidor NTP quien se encargará de actualizar y mantener sincronizada la hora y fecha en el router 1 a cien se configuro como cliente de este servicio.

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

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

Tabla 38. Parámetros de acceso en líneas VTY

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 172.16.1.0 0.0.0.3
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)#transport input telnet

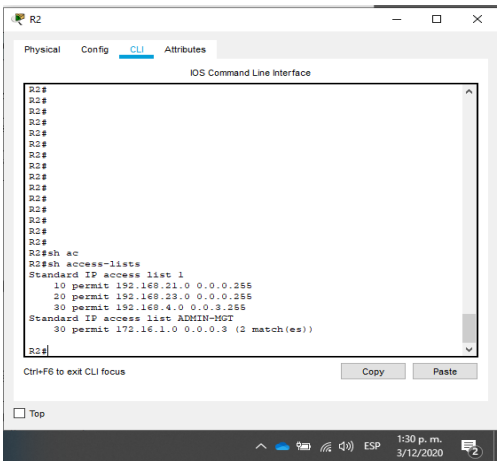
Verificar que la ACL funcione como se espera, se realiza conexión telnet desde R1 a R2.	Figura 59. Conexión telnet desde R1 a R2 

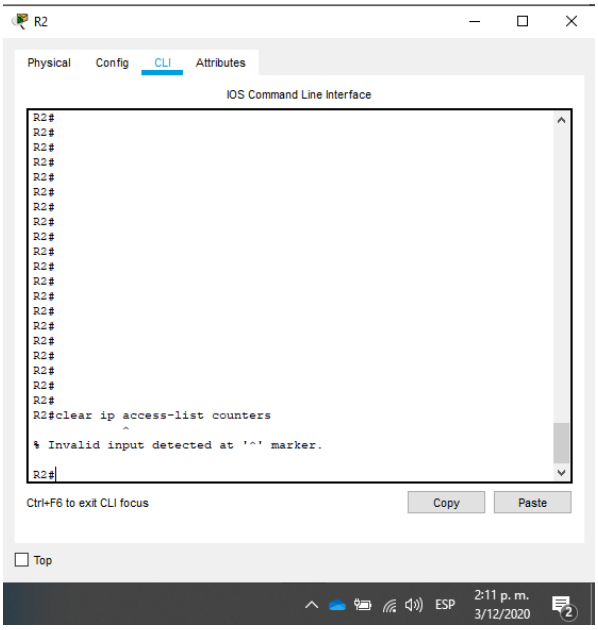
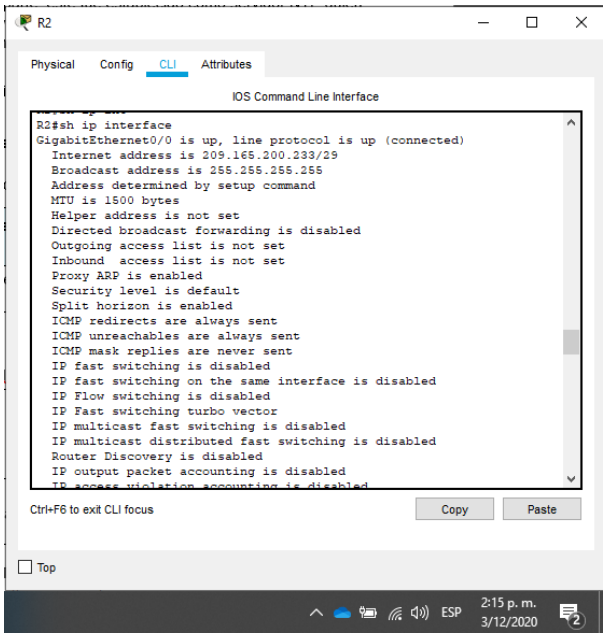
Fuente: Autor

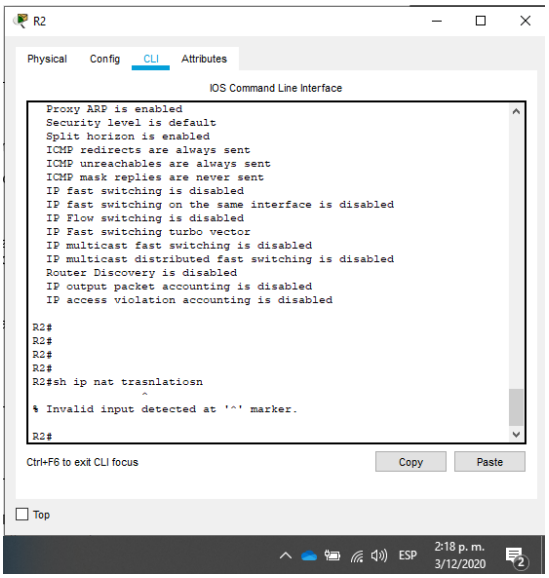
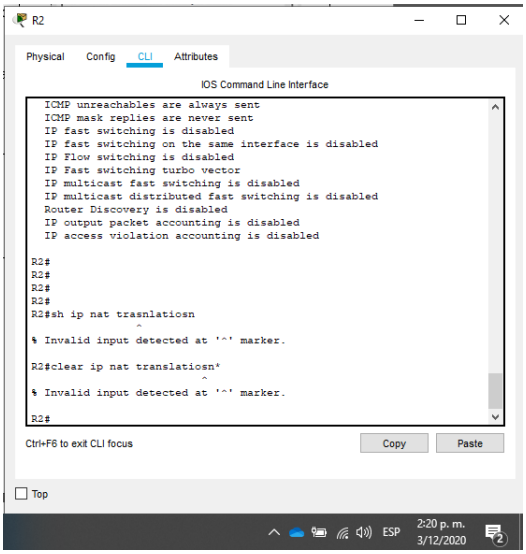
Al haber ejecutado los comandos anteriores, se creó una lista de acceso que fue asignada a las líneas vty del router 2, para que solo le permita el ingreso vía telnet desde el router 1, los demás equipos no podrán ingresar por este medio.

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

Tabla 39. Verificación de parámetros de configuración en R2

Descripción del comando	Resultado
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció **RTA**: con el comando **show access-lists**	Figura 60. Ejecución comando show access-list 

Restablecer los contadores de una lista de acceso **RTA**: con el comando **clear ip acces-list counters**	Figura 61. Ejecución de comando clear ip acces-list counters  *Comando no soportado por Packet Tracer
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? **RTA**: con el comando **show ip interface**	Figura 62. Ejecución de comando Show ip interface  *Comando no soportado por Packet Tracer

¿Con qué comando se muestran las traducciones NAT? **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. **RTA**: Con el comando **show ip nat translations**	Figura 63. Ejecución de comando show ip nat translations  *Comando no soportado por Packet Tracer
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? **RTA**: con el comando **clear ip nat translation ***	Figura 64. Ejecución de comando clear ip nat trasnlations  *Comando no soportado por Packet Tracer

Fuente: Autor

Por medio de los anteriores comandos se puede verificar el estado de los servicios tales como NAT, ACL, contadores ACL y su reinicio.

CONCLUSIONES

Se concluye que, mediante el uso del servicio de DHCP, los dispositivos pueden obtener parámetros tales como dirección IP, mascara de red, puerta de enlace y DNS, adicionalmente, se reconoce la posibilidad de establecer exclusión de rangos de direcciones que no serán utilizados en el direccionamiento que se distribuye de forma automática a los dispositivos finales.

Por medio de la configuración de Etherchannel, se permite agrupar hasta 16 enlaces troncales diferentes, el propósito de su uso consiste en sumar sus capacidades para el transporte de información, cuya ventaja se traduce en mayor capacidad de transporte de información y redundancia en los enlaces disponibles por ruta.

Se reconoce la importancia de la configuración de subinterfaces mediante la encapsulación Dot1Q, ya que al implementar esta alternativa se reduce la necesidad de adquirir e instalar más dispositivos para la integración de nuevas redes, logrando de esta manera optimizar los recursos existentes; lo que también permite disminuir los costos de implementación de la red.

Sin duda, se establece que el uso de VLAN’s es la manera eficiente de segmentar la red, se concluye que, mediante su uso, incrementa rendimiento y disminuye la difusión de broadcast innecesario en la red. También permite agrupar los dispositivos que tienen un uso común facilitando su administración gestión general.

Para culminar, se reconoce que el protocolo de enrutamiento OSPF es uno de los más eficientes entre los protocolos de enrutamiento dinámico, ya que este mantiene actualizadas todas las rutas disponibles entre dispositivos que componen el área. Este protocolo evalúa características tales como el ancho de banda y congestión que ruta posee; a fin de hacer la selección de la mejor ruta para transmitir.

BIBLIOGRAFÍA

CISCO. Redes Conmutadas. Principios de Enrutamiento y Conmutación. {En línea}. {Consultado octubre 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. Routing Estático. Principios de Enrutamiento y Conmutación. {En línea}. {Consultado octubre 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. VLAN. Principios de Enrutamiento y Conmutación. {En línea}. {Consultado octubre 2020}. Disponible en https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

ICONTEC INTERNATIONAL. EL COMPENDIO DE TESIS Y OTROS TRABAJOS DE GRADO. {En línea}. {Consultado junio 2009}. Disponible en: http://www.ICONTEC.org/BancoConocimiento/C/compendio_de_tesis_y_otros_trabajos_de_grado/compendio_de_tesis_y_otros_trabajos_de_grado.asp?CodIdioma=ESP.

UNAD. Principios de Enrutamiento [OVA]. {En línea}. {Consultado octubre 2020}. Disponible en https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. Configuración de EtherChannel y enlace troncal 802.1Q entre switches de configuración fija Catalyst L2 y un enrutador (enrutamiento InterVLAN). {En línea}. {30 agosto de 2005} Disponible en https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

PÉREZ TORRES. Daniel. Redes Cisco curso práctico para la certificación CCNA. 7 ed. Madrid: Alfaomega, 2018. 588p.

ANEXOS

ANEXO 1 Archivo de simulación

https://drive.google.com/drive/folders/1eVSr7NUOAtHQeUnyFMPyeuVVH3FbjcMq?usp=sharing

ANEXO 2 Articulo científico

https://drive.google.com/drive/folders/1eVSr7NUOAtHQeUnyFMPyeuVVH3FbjcMq?usp=sharing