SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JOSÉ JULIÁN RAMÍREZ LONDOÑO

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

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JOSÉ JULIÁN RAMÍREZ LONDOÑO

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

Presentado al DIRECTOR: Ing. JUAN CARLOS VESGA FERREIRA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

ARMENIA, 11 de diciembre de 2020

AGRADECIMIENTOS

A Dios que me brinda la oportunidad de perseverar en los objetivos planteados en mi vida, a mi familia que me han apoyado incondicionalmente en este proceso y a mi compañera de vida que me ha dado aliento para no desfallecer ante las dificultades.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

NAT (Network Address Translation): Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

DHCP (Dynamic Host Configuration Protocol): “Protocolo de Configuración Dinámica de Servidor. Se trata de un protocolo cliente-servidor que permite que una o más máquinas obtengan su configuración de red de manera totalmente automática.” (Pastor, 2009)
.
LAN: Son las siglas de "Local Area Network", es decir, Red de área local. Una Red LAN conecta diferentes ordenadores en un área pequeña, como un edificio o una habitación, lo que permite a los usuarios enviar, compartir y recibir archivos

ROUTING: Proceso de determinar el mejor camino para realizar el encaminamiento. En otras palabras, routing es el proceso que se realiza para determinar las tablas de encaminamiento.

EIGRP (Enhanced Interior Gateway Routing Protocol): Es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace.

OSPF (Open Shortest Path First): Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.
PACKET TRACERT: Herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

ROUTER: Dispositivo de hardware que permite la interconexión de ordenadores en red. Este dispositivo es el encargado de distribuir la conexión a Internet a distintos computadores vinculados a una misma red local actuando como un puente entre nuestros dispositivos y la internet.

CCNA (Cisco Certified Network Associate): Es un plan de capacitación en tecnología de redes informáticas que la empresa Cisco ofrece.

RESUMEN

Esta actividad que corresponde a la entrega del informe final contiene dos escenarios los cuales proponen utilizar todos los aspectos técnicos vistos a lo largo del diplomado de profundización, además permite afianzar los conocimientos mediante la simulación de todos los comandos en los dispositivos que conformación la red de cada escenario y sus correspondientes parámetros.

Palabras clave: CISCO, CCNA, EtherChannel, Conmutación, Enrutamiento, Redes, Electrónica, Port-Security.

ABSTRACT

This activity, which corresponds to the delivery of the final report, contains two scenarios which propose to use all the technical aspects seen throughout the in-depth diploma course, in addition to consolidating knowledge by simulating all the commands in the devices that make up the network of each scenario and its corresponding parameters.

Keywords: CISCO, CCNA, EtherChannel, Routing, Switching, Networking, Electronics, Port-Security.

INTRODUCCIÓN

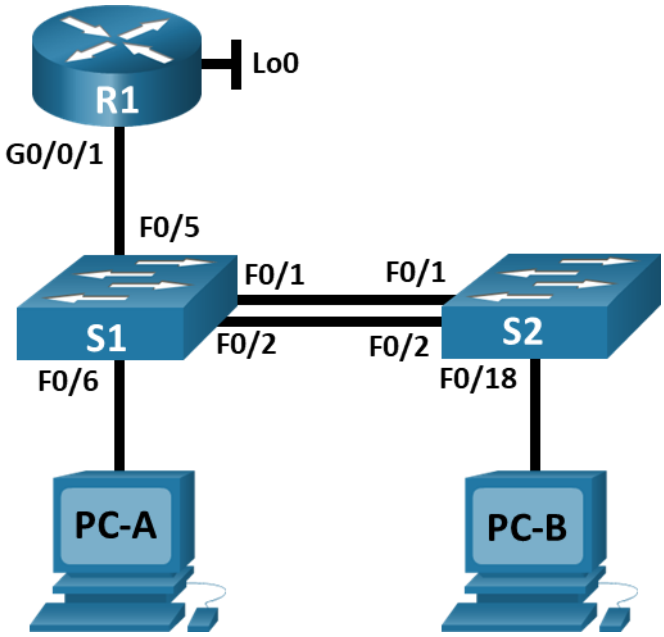
Este trabajo muestra el resultado de lo aprendido en el transcurso del diplomado de CISCO, contiene todos los elementos técnicos que se vieron durante los temas tratados en este diplomado de profundización. Este laboratorio fue desarrollado mediante el simulador packet tracer en donde podemos encontrar el funcionamiento real de cada uno de los escenarios planteados.

DESARROLLO

ESCENARIO 1

Escenario 1

FIGURA 1 ESCENARIO 1



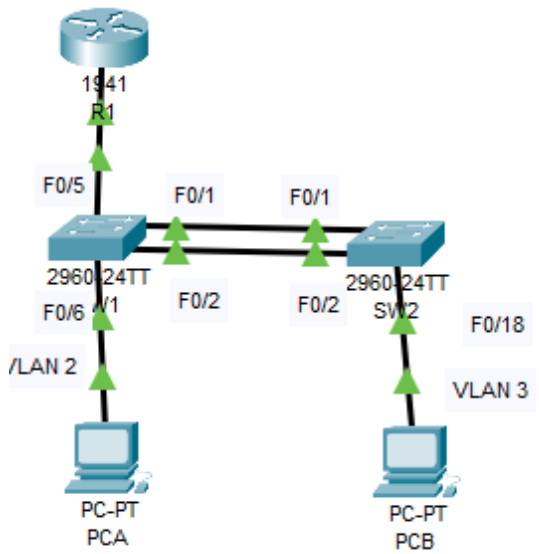
En La *figura 1*, se contempla toda la topología del escenario que se va a configurar, la cual se compone de dos Switch, 1 router y dos PC de escritorio, para que los Switch soporten ipv4 - ipv6 se realiza una actualización del ios adicional. Adicionalmente se realizan los procedimientos para la conexión entre S1 al PC-A, S2 al PC-B, R1 al S1, S2 al S1 y S2 al S1. Se procede a la configuración de cada uno de los componentes.

En la siguiente *tabla 1* se encuentran las Vlan que se procede a la configuración como redes independientes dentro de la red del escenario 1.

TABLA 1 NOMBRES VLAN

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

FIGURA 2. SIMULACIÓN DE ESCENARIO 1



1.1 Asignación de direcciones

Se asignan direcciones ip a cada una de las VLAN además de, (Switch 1, Switch 2), (Router 1), (PCA y PCB) para permitir la conexión entre los dispositivos de la red.

TABLA 2 ASIGNACIÓN DE DIRECCIONES.

Dispositivo / interfaz	Dirección IP / Prefijo	Comandos y configuración de la Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	R1(config)# interface g0/0/1 R1(config-if)# description Conexion a SW1 R1(config-if)# no shutdown R1(config-if)# exit R1(config)# interface g0/1.2 R1(config-subif)# description Red Bikes R1(config-subif)# encapsulation dot1q 2 R1(config-subif)# ip address 10.19.8.1 255.255.255.192 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Comandos y configuración de la Puerta de enlace predeterminada
R1 G0/0/1.3	10.19.8.65 /27	R1(config)# interface g0/1.3 R1(config-subif)# description Red Trikes R1(config-subif)# encapsulation dot1q 3 R1(config-subif)# ip address 10.19.8.65 255.255.255.224 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# ipv6 address 2001:db8:acad:b: :1 /64
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	R1(config)# interface g0/1.4 R1(config-subif)# description Red Management R1(config-subif)# encapsulation dot1q 4 R1(config-subif)# ip address 10.19.8.97 255.255.255.248 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# ipv6 address 2001:db8:acad:c: :1 /64
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Comandos y configuración de la Puerta de enlace predeterminada
R1 G0/0/1.6	No corresponde	R1(config)# interface g0/1.6 R1(config-subif)# description Red Native R1(config-subif)# encapsulation dot1q 6 native
R1 Loopback0	209.165.201.1 /27	R1(config)# interface loopback0 R1(config-if)# ip address 209.165.201.1 255.255.255.224 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# ipv6 address 2001:db8:acad:209::1/64 R1(config-if)# description loopback adapter R1(config-if)# no shutdown R1(config-if)# exit
R1 Loopback0	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

Dispositivo / interfaz	Dirección IP / Prefijo	Comandos y configuración de la Puerta de enlace predeterminada
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

1.2 Inicializar, recargar y configurar aspectos básicos de los dispositivos.

Se comienza con la puesta a punto del router y switch, haciendo eliminación de cualquier configuración antigua.

1.2.1 Inicializar y volver a cargar el router y el switch.

Recargando el switch, se configura la plantilla SDM para que admita IPv6 y se vuelve a cargar el switch, esto se realiza mediante los siguientes comandos:

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Se usa el comando siguiente que muestra las características de la plantilla SDM:

```
S1#show sdm prefer
 The current template is "dual-ipv4-and-ipv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.
```

number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0
number of IPv6 multicast groups: 0.375k
number of directly-connected IPv6 addresses: 0
number of indirect IPv6 unicast routes: 0
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.125K
number of IPv4/MAC security aces: 0.375K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.625k
number of IPv6 security aces: 0.125K

1.2.2 Configuración R1.

En la siguiente *tabla 3* comienza con la configuración básica del dispositivo R1, así como también las especificación y comandos de configuración.

TABLA 3. CONFIGURACIÓN R1

Tarea	Especificaciones y comandos de configuración
Desactivar la búsqueda DNS, para iniciar la configuración de R1.	R1(config)#no ip domain-lookup
Asignación nombre del router “R1”	R1 Router#conf t Router(config)#hostname R1 R1(config)#
Asignación de nombre de dominio ccna-lab.com	ccna-lab.com R1(config)#ip domain name ccna-lab.com
Se asigna “ciscoenpass” como contraseña cifrada para el modo EXEC privilegiado.	Ciscoenpass R1(config)#enable secret ciscoenpass

Tarea	Especificaciones y comandos de configuración
Se asigna “ciscoonpass” como contraseña de acceso a la consola	Ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#exec-timeout 4 0 R1(config-line)#login
Se delimita a 10 digitos la longitud mínima de las contraseñas	R1(config)#security passwords min-length 10 10 caracteres
Se crea un usuario administrativo en la base de datos local y se establece contraseña de acceso.	Nombre de usuario: admin Password: admin1pass R1(config)# username admin secret admin1pass
Se Configura el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#password ciscoconpass R1(config-line)#exec-timeout 4 0 R1(config-line)#transport input ssh R1(config-line)#login local
Se configura VTY solo aceptando SSH	
Se realiza la configuración del cifrado de las contraseñas.	R1(config)# service password-encryption
Se configura el mensaje de MOTD para indicar acceso no autorizado.	R1(config)#banner motd $ ACCESO RESTRINGIDO - SOLO USUARIOS AUTORIZADOS $
Se Habilita el routing IPv6	R1(config)#ipv6 unicast-routing
Se configura la interfaz G0/0/1	Establezca la descripción R1(config)#interface g0/1 R1(config-if)#description Conexion a SW1 R1(config-if)# no shutdown R1(config-if)#exit Establece la dirección IPv4.

Tarea	Especificaciones y comandos de configuración
	Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6. Activar la interfaz.
Se configura la interfaz de Loopback0 para la conexión a internet de la red.	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1
Se configura una clave de cifrado RSA	Módulo de 1024 bits R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK] R1(config)#

1.2.3 Configuración de los switch (S1 y S2).

Se realiza la configuración para la actualización IOS de los dos switch, permitiendo pasar de la versión 12 a la 15. Se realiza conectando un servidor a cada switch el cual contiene la imagen, se realiza con los siguientes comandos.

```
c2960-lanbasek9-mz.150-2.SE4.bin
S1#copy tftp: flash:
Address or name of remote host []? 192.168.0.10
Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin
Destination filename [c2960-lanbasek9-mz.150-2.SE4.bin]?

Accessing tftp://192.168.0.10/c2960-lanbasek9-mz.150-2.SE4.bin...
Loading c2960-lanbasek9-mz.150-2.SE4.bin from 192.168.0.10:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4670455 bytes]

4670455 bytes copied in 0.112 secs (3352568 bytes/sec)
S1#dir
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    8  -rw-     4670455          <no date>  c2960-lanbasek9-mz.150-2.SE4.bin
    7  -rw-        1553          <no date>  config.text
    6  -rw-         616          <no date>  vlan.dat

S1(config)#boot system c2960-lanbasek9-mz.150-2.SE4.bin
S1#copy run sta
Destination filename [startup-config]?
Building configuration...
[OK]
S1#reload
```

A continuación, se realiza la configuración de seguridad básica de los switch. Además, se configuran las líneas vty (Las líneas VTY son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones y estas son virtuales, son una funcionan mediante software.

TABLA 4 CONFIGURACIÓN S1

Tarea	Especificaciones y comandos de configuración
Se realiza la desactivación de la búsqueda DNS.	Switch(config)#no ip domain-lookup
Se asigna el nombre del switch	Switch(config)#hostname S1
Se asigna el dominio ccna-lab.com	ccna-lab.com S1(config)#ip domain name ccna-lab.com
Se configura la contraseña cifrada para el modo EXEC privilegiado como “ciscoenpass”	S1(config)#enable secret ciscoenpass
Se establece la contraseña de acceso a la consola “ciscoconpass”	Ciscoconpass S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#exec-timeout 4 0 S1(config-line)#login
Se realiza la creación de un usuario administrativo en la base de datos local admin y admin1pass como contraseña.	Nombre de usuario: admin Password: admin1pass S1(config)#username admin secret admin1pass
Se realiza la configuración el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S1(config-line)#password ciscoconpass S1(config-line)#exec-timeout 4 0 S1(config-line)#transport input ssh S1(config-line)#login local
Se configuran las líneas VTY para que acepten únicamente las conexiones SSH	
Se configuran las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Se configura un MOTD Banner para prevenir el acceso no autorizado.	S1(config)#banner motd $ ACCESO RESTRINGIDO SOLO USUARIOS AUTORIZADOS $
Se establece una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com

Tarea	Especificaciones y comandos de configuración
	Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Se realiza la configuración de la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 S1# configure terminal S1(config)# vlan 4 S1(config-vlan)# exit S1(config)# interface vlan 4 %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down 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
Se configura la puerta de enlace predeterminada.	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)# ip default-gateway 10.19.8.97

TABLA 5. CONFIGURACIÓN S2

Tarea	Especificaciones y comandos de configuración
Se realiza la desactivación de la búsqueda DNS.	Switch(config)#no ip domain-lookup
Se asigna el nombre del switch	Switch(config)#hostname S2
Se asigna el dominio ccna-lab.com	ccna-lab.com S2(config)#ip domain name ccna-lab.com
Se configura la contraseña cifrada para el modo EXEC privilegiado como “ciscoenpass”	Ciscoenpass S2(config)#enable secret ciscoenpass
Se establece la contraseña de acceso a la consola “ciscoconpass”	Ciscoconpass S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#exec-timeout 4 0 S2(config-line)#login
Se realiza la creación de un usuario administrativo en la base de datos local admin y admin1pass como contraseña.	Nombre de usuario: admin Password: admin1pass S2(config)#username admin secret admin1pass
Se realiza la configuración el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 S2(config-line)#password ciscoconpass S2(config-line)#exec-timeout 4 0 S2(config-line)#transport input ssh S2(config-line)#login local
Se configuran las líneas VTY para que acepten únicamente las conexiones SSH	
Se configuran las contraseñas de texto no cifrado	S2(config-line)#service password-encryption
Se configura un MOTD Banner para prevenir el acceso no autorizado.	S2(config)#banner motd $ ACCESO RESTRINGIDO SOLO USUARIOS AUTORIZADOS $

Tarea	Especificaciones y comandos de configuración
Se establece una clave de cifrado RSA	Módulo de 1024 bits S2(config)#crypto key generate rsa The name for the keys will be: S1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Se realiza la configuración de la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 S1# configure terminal S1(config)# vlan 4 S1(config-vlan)# exit S1(config)# interface vlan 4 %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down S1(config-if)# ip address 10.19.8.99 255.255.255.248 S1(config-if)# ipv6 address 2001:db8:acad:c: :99 /64 S1(config-if)# ipv6 address fe80: :98 link-local S1(config-if)# no shutdown S1(config-if)# exit
Se configura la puerta de enlace predeterminada.	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S2(config)# ip default-gateway 10.19.8.97

1.3 configuración de la infraestructura de red (VLAN,Trnking, Ether Channel).

1.3.1 Configuración estructura de red del S1.

Se realiza creación de las VLAN en los Switch, también creación del modo trunk y el grupo de puertos EtherChannel de Capa 2 que usa las interfaces F0/1 y F0/2. Además, configuración del puerto de acceso de host para VLAN 2, configuración de la seguridad en los puertos de acceso.

TABLA 6. CONFIGURACIÓN ESTRUCTURA DE RED DEL DISPOSITIVO S1

Tarea	Especificación y comandos de configuración
Se realiza la creación de las VLAN de la red, para su correcto funcionamiento.	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native S1(config)# vlan 2 S1(config-vlan)# name Bikes S1(config-vlan)# vlan 3 S1(config-vlan)# name Trikes S1(config-vlan)# vlan 4 S1(config-vlan)# name Management S1(config-vlan)# vlan 5 S1(config-vlan)# name Parking S1(config-vlan)# vlan 6 S1(config-vlan)# name Native S1(config-vlan)# end

Tarea	Especificación y comandos de configuración
Se crean los enlaces troncales 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5 S1(config)# interface f0/1 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 6 S1(config)# interface f0/2 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 6 S1(config)# interface f0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 6
Se crean 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 f0/1-2 S1(config-if-range)# channel-group 1 mode active S1(config-if-range)# exit
Se realiza la configuración el puerto de acceso de host para VLAN 2. Para la interfaz F0/6	Interface F0/6 S1(config)# interface f0/6 S1(config-if)# switchport mode access S1(config-if)# switchport access vlan 2
Se asigna y configura la seguridad del puerto para los puertos de acceso.	Permitir 3 direcciones MAC S1(config)# interface f0/6 S1(config-if)# switchport port-security S1(config-if)# switchport port-security maximum 3

Tarea	Especificación y comandos de configuración
	S1(config-if)# switchport port-security violation restrict S1(config-if)# switchport port-security aging time 60 S1# show port-security interface f0/6
Se realiza el apagado de las interfaces que no se utilizan como mecanismo de seguridad y protección.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar F0/3- S1(config)#interface f0/3 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 5 S1(config-if)#description PTO PROTEGIDO SIN USO F0/4 proteger S1(config)#interface f0/4 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 5 S1(config-if)#description PTO PROTEGIDO SIN USO Fo/7 – f0/24 proteger S1(config)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description PTO PROTEGIDO SIN USO S1(config-if-range)#shutdown G0/1-G0/2 S1(config-if)#interface range g0/1-2 S1(config-if-range)#switchport mode access

Tarea	Especificación y comandos de configuración
	S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown

1.3.2 Configuración estructura de red del S2.

TABLA 7. CONFIGURACIÓN ESTRUCTURA DE RED DEL DISPOSITIVO S2

Tarea	Especificación
Se realiza la creación de las VLAN de la red, para su correcto funcionamiento.	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native S2(config)# vlan 2 S2(config-vlan)# name Bikes S2(config-vlan)# vlan 3 S2(config-vlan)# name Trikes S2(config-vlan)# vlan 4 S2(config-vlan)# name Management S2(config-vlan)# vlan 5 S2(config-vlan)# name Parking S2(config-vlan)# vlan 6 S2(config-vlan)# name Native S2(config-vlan)# end
Se crean los enlaces troncales 802.1Q que	Interfaces F0/1 y F0/2 S2(config)# interface f0/1

Tarea	Especificación
utilicen la VLAN 6 nativa	S2(config-if)# switchport mode trunk S2(config-if)# switchport trunk native vlan 6 S2(config)# interface f0/2 S2(config-if)# switchport mode trunk S2(config-if)# switchport trunk native vlan 6
Se crean 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 f0/1-2 S2(config-if-range)# channel-group 1 mode active S2(config-if-range)# exit
Se realiza la configuración el puerto de acceso de host para VLAN 3. Para la interfaz F0/18	Interfaz F0/18 S2(config)# interface f0/18 S2(config-if)# switchport mode access S2(config-if)# switchport access vlan 3
Se asigna y configura la seguridad del puerto para los puertos de acceso.	permite 3 MAC addresses S2(config)# interface f0/18 S2(config-if)# switchport port-security S2(config-if)# switchport port-security maximum 3 S2(config-if)# switchport port-security violation restrict S2(config-if)# switchport port-security aging time 60 S2# show port-security interface f0/18
Se realiza el apagado de las interfaces que no se utilizan como	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Tarea	Especificación
mecanismo de seguridad y protección.	F0/3-17 S2(config)#interface range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description PTO PROTEGIDO SIN USO S2(config-if-range)#shutdown F0/19-24 S2(config)#interface range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description PTO PROTEGIDO SIN USO S2(config-if-range)#shutdown G0/1-G0/2 S2(config-if)#interface range g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown

1.4 Configurar soporte de host.

1.4.1 Configuracion R1

TABLA 8. CONFIGURACIÓN SOPORTE DE HOST EN EL DISPOSITIVO R1

Tarea	Especificación y comandos de configuración
Se realiza la configuración 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 loopback0 R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 R1#show ip route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is 0.0.0.0 to network 0.0.0.0 10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks C 10.19.8.0/26 is directly connected, GigabitEthernet0/1.2 L 10.19.8.1/32 is directly connected, GigabitEthernet0/1.2 C 10.19.8.64/27 is directly connected, GigabitEthernet0/1.3 L 10.19.8.65/32 is directly connected, GigabitEthernet0/1.3 C 10.19.8.96/29 is directly connected, GigabitEthernet0/1.4 L 10.19.8.97/32 is directly connected, GigabitEthernet0/1.4

Tarea	Especificación y comandos de configuración
	209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks C 209.165.201.0/27 is directly connected, Loopback0 L 209.165.201.1/32 is directly connected, Loopback0 S* 0.0.0.0/0 is directly connected, Loopback0
Se configura IPv4 DHCP para la 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 Red 10.19.8.0 / 26 Rango hosts 10.19.8.1 - 10.19.8.62 Broadcast 10.19.8.63 EXCLUDE 10.19.8.1 - 10.19.8.51 DHCP POOL INICIAL 10.19.8.52 DHCP POOL FINAL 10.19.8.62 GATEWAY 10.19.8.1 Mask 255.255.255.192 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.51 R1(config)#ip dhcp pool R1_DHCP_VLAN2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net

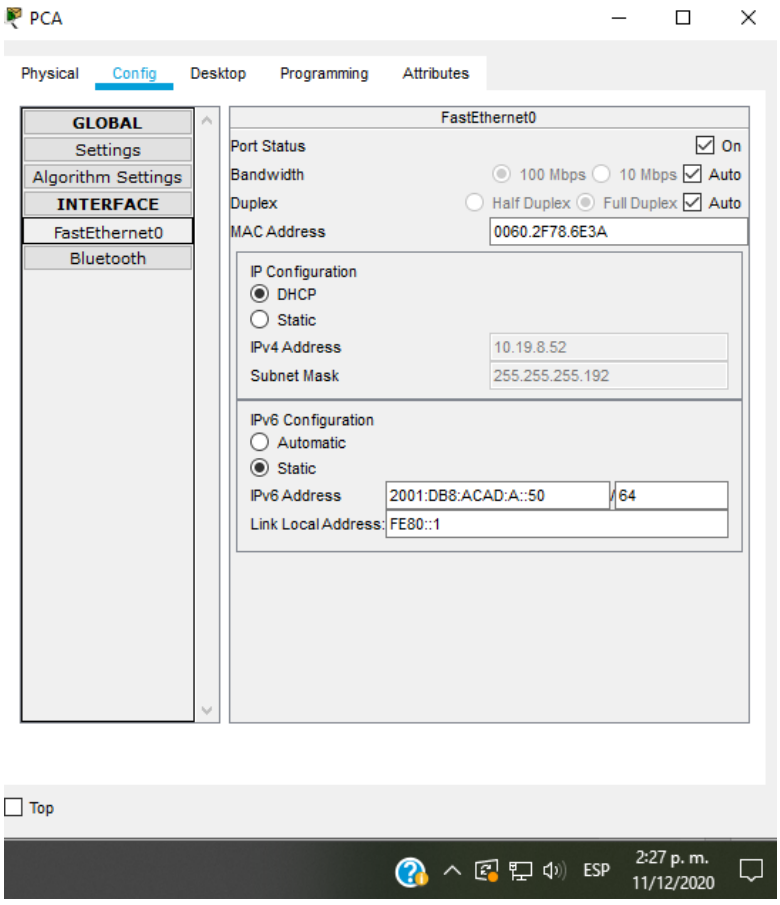
Tarea	Especificación y comandos de configuración
Se realiza la configuración DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada Red 10.19.8.64 Mask 255.255.255.224 Rango hosts 10.19.8.65 - 10.19.8.94 Broadcast 10.19.8.95 EXCLUDE 10.19.8.65 - 10.19.8.83 DHCP POOL INICIAL 10.19.8.84 DHCP POOL FINAL 10.19.8.94 GATEWAY 10.19.8.65 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.83 R1(config)#ip dhcp pool R1_DHCP_VLAN3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net

1.5 Configuración de los servidores

TABLA 9. CONFIGURACIÓN DE RED DE PC-A

PC-A Network Configuration	
Descripción	ccna-a.net
Dirección física	DHCP
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

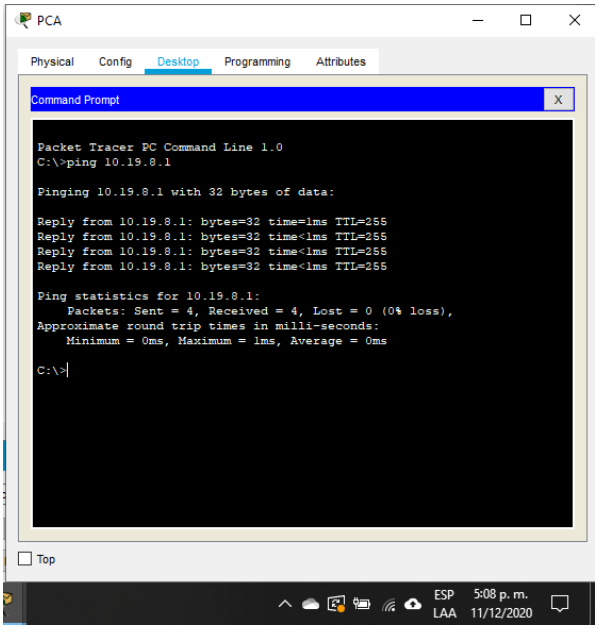
FIGURA 3 CONFIGURACIÓN IP PC-A

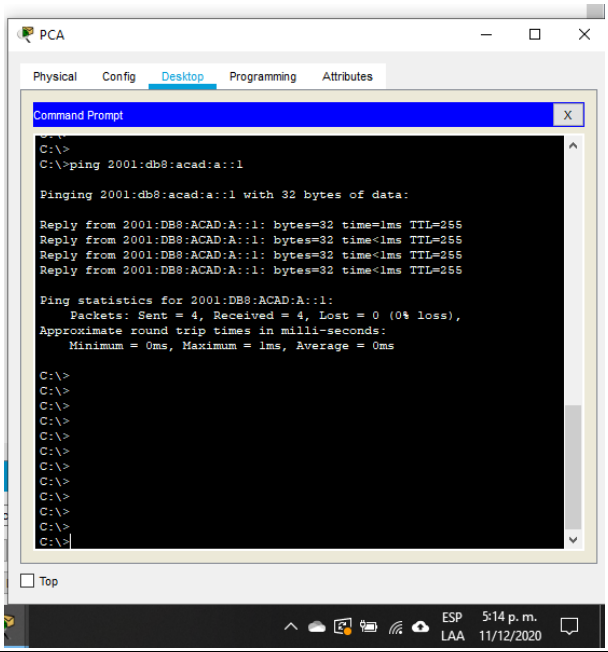
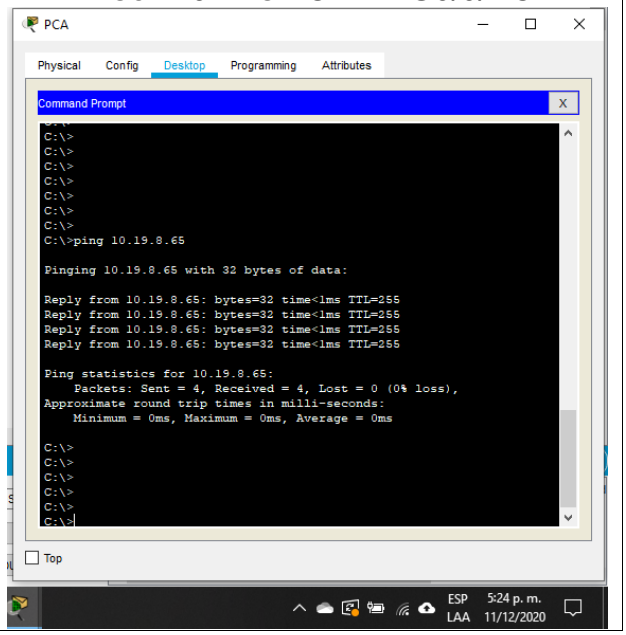


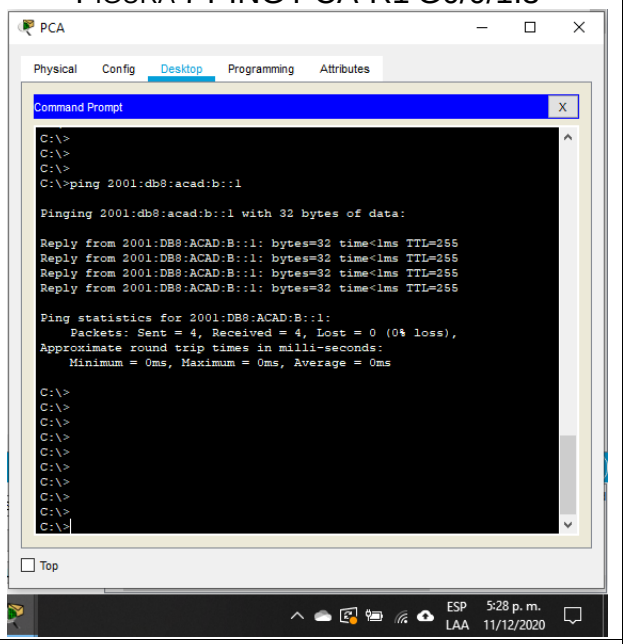
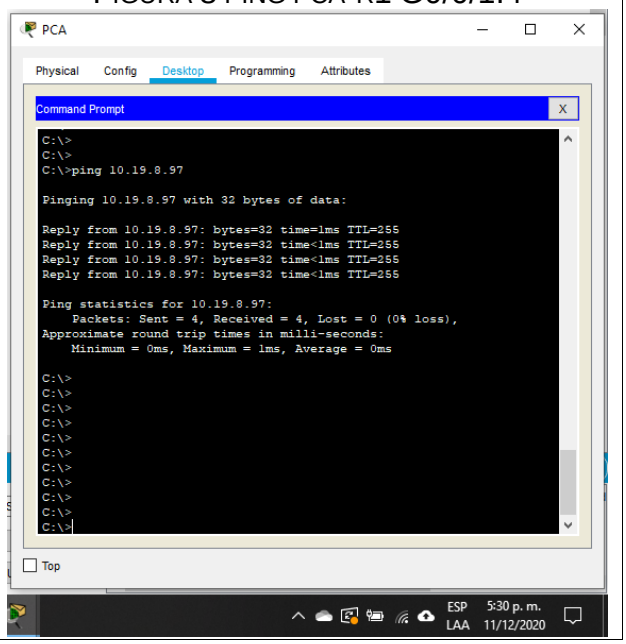
En esta figura se puede reconocer la respuesta y asignación automática de la dirección ip mediante la conexión DHCP para ipv4, además de la configuración para ipv6.

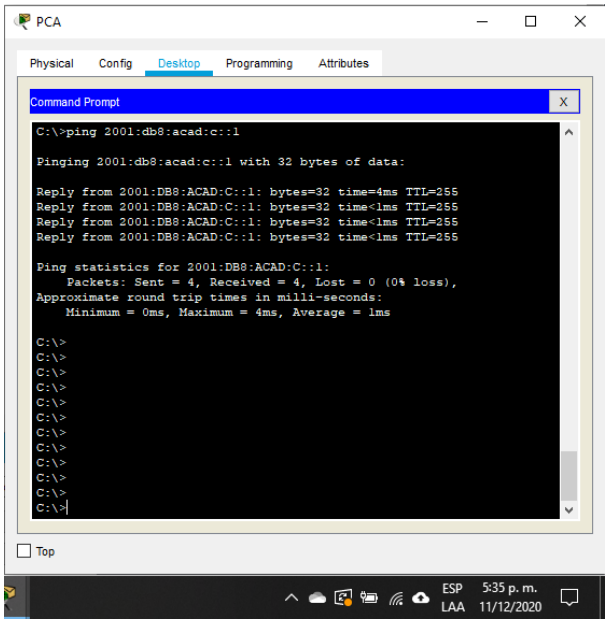
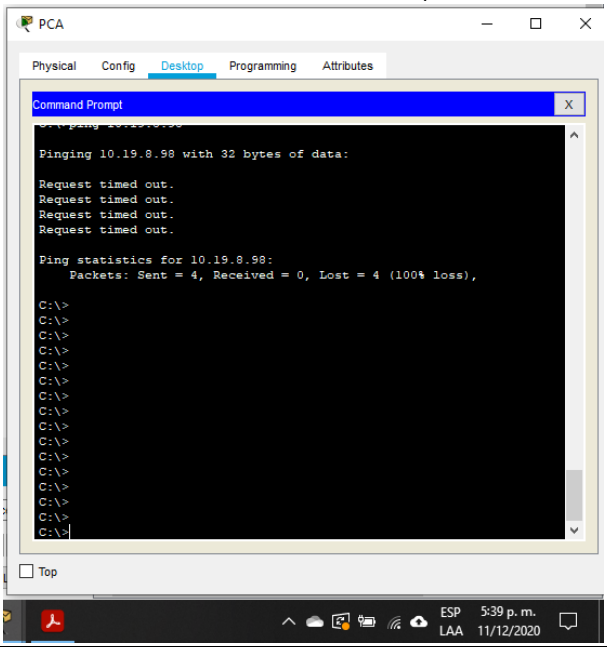
1.6 Probando la conectividad de la red

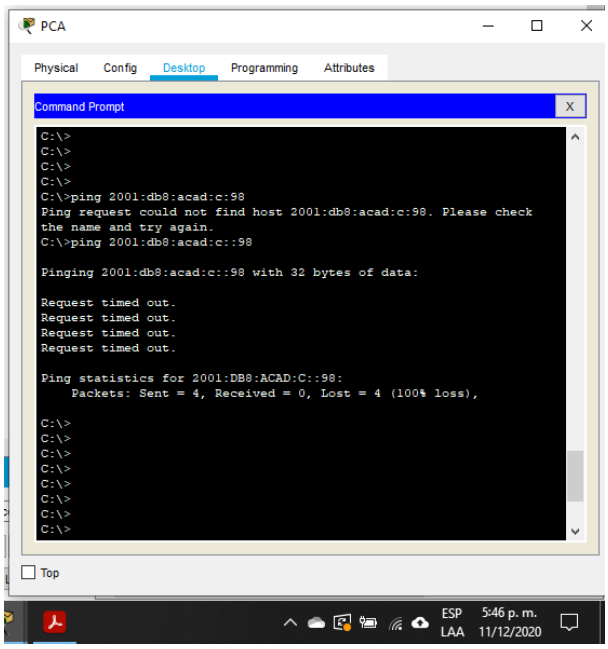
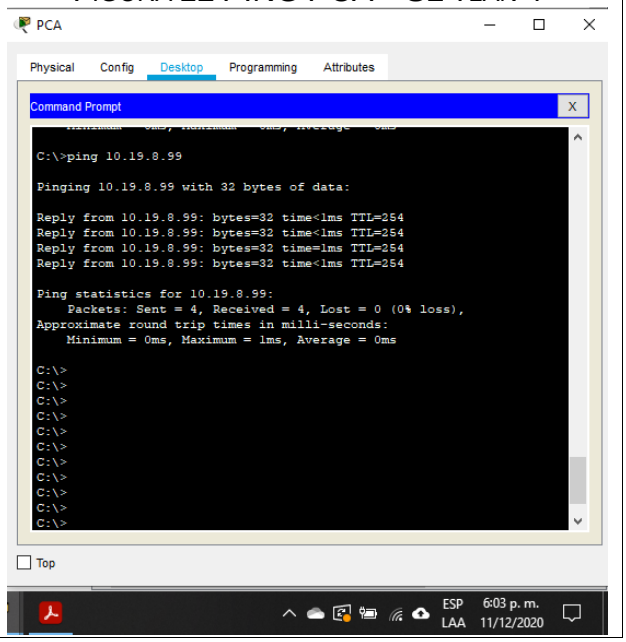
TABLA 10. PROBANDO LA CONECTIVIDAD DE LA RED.

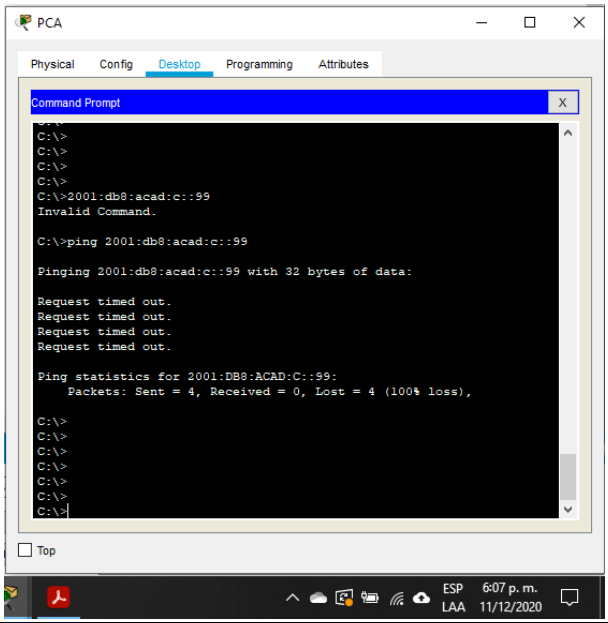
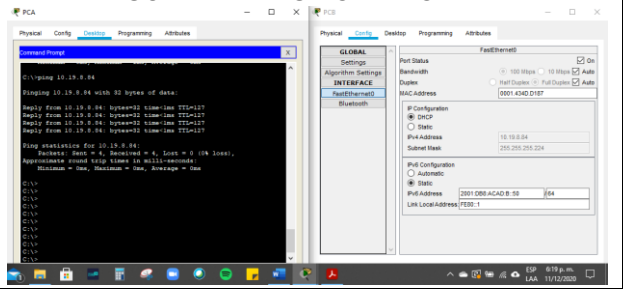
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	FIGURA 4 PING PCA – R1 G0/0/1.2 

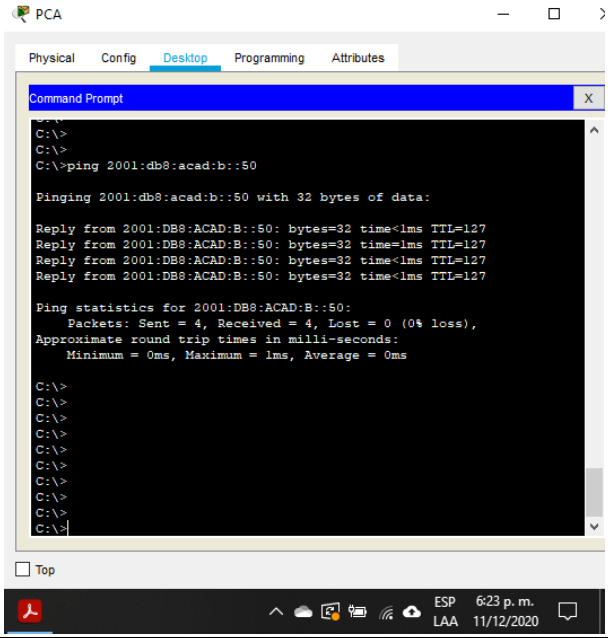
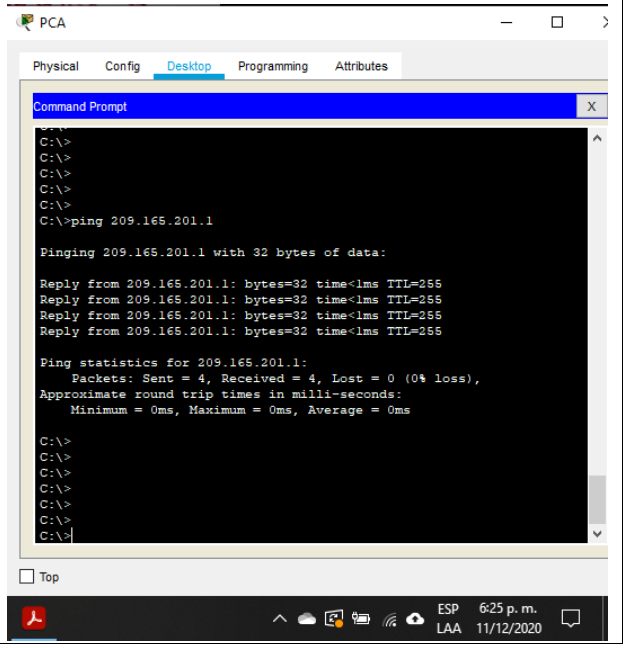
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:a::1	FIGURA 5 PING PCA – R1 G0/0/1.2 
	R1, G0/0/1.3	Dirección	10.19.8.65	FIGURA 6 PING PCA-R1 G0/0/1.3 

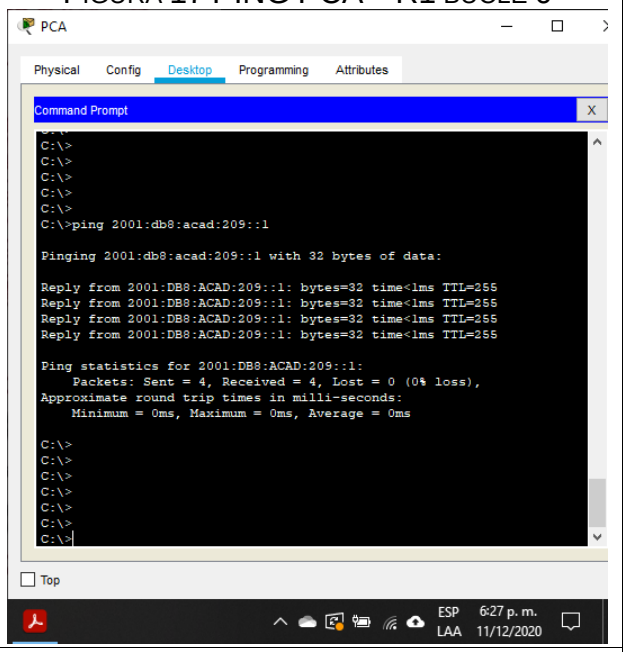
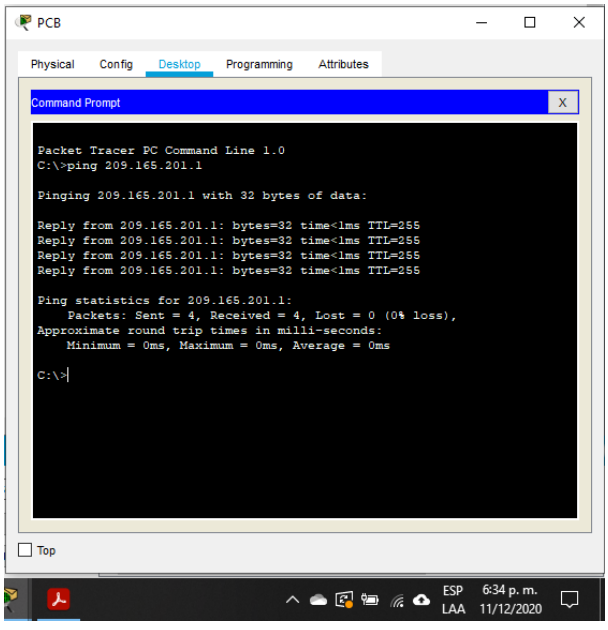
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b::1	FIGURA 7 PING PCA-R1 G0/0/1.3 
	R1, G0/0/1.4	Dirección	10.19.8.97	FIGURA 8 PING PCA-R1 G0/0/1.4 

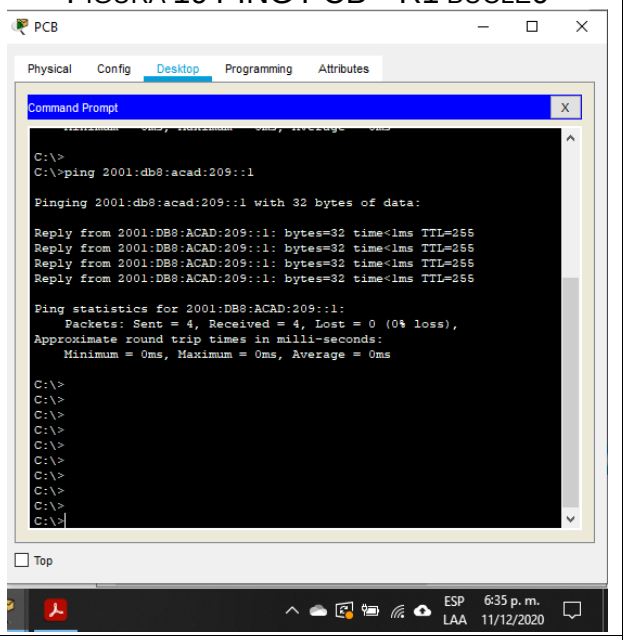
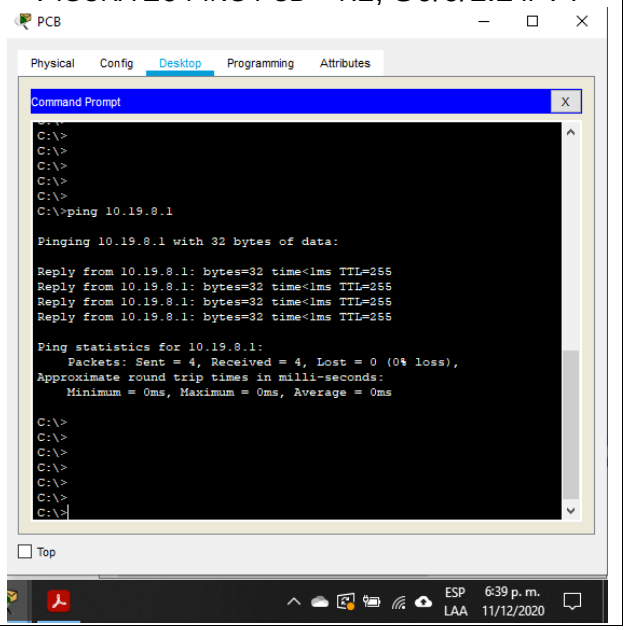
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A		IPv6	2001:db8:acad:c::1	FIGURA 9 PING PCA-R1 G0/0/1.4 
	S1, VLAN 4	Dirección	10.19.8.98	FIGURA 10 PING PCA – S1, VLAN 4 

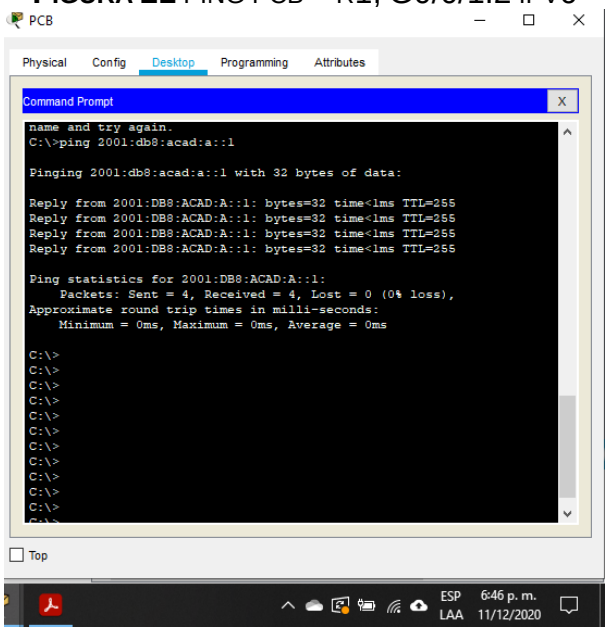
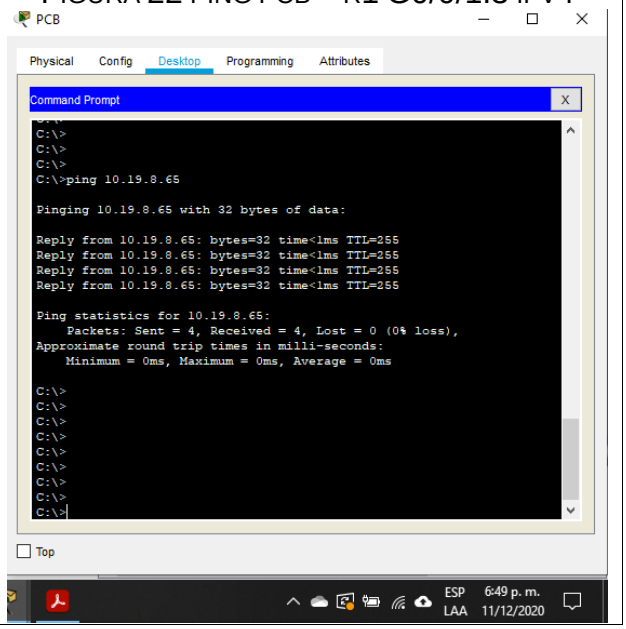
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c::98	FIGURA 11 PING PCA – S1 VLAN4 
	S2, VLAN 4	Dirección	10.19.8.99	FIGURA 12 PING PCA – S2 VLAN 4 

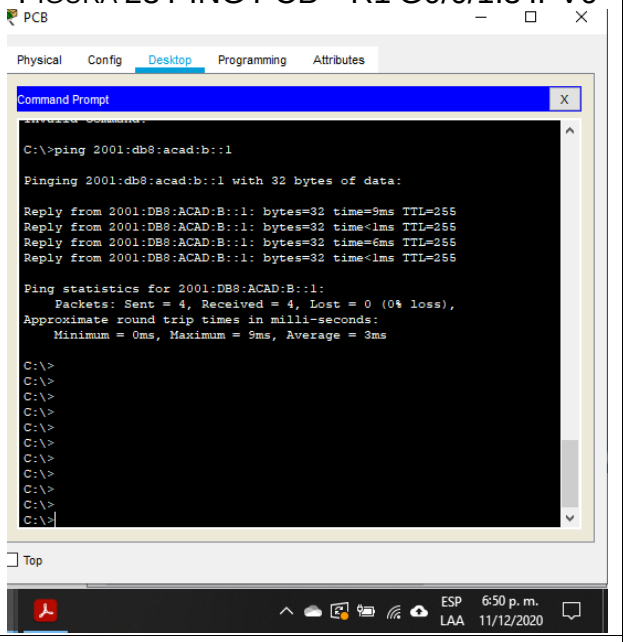
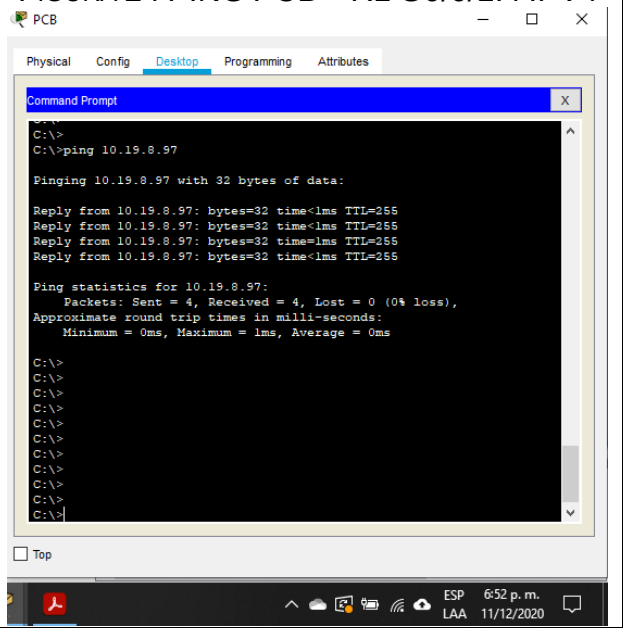
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c::99	FIGURA 13 PING PCA – S2 VLAN 4 
	PC-B	Dirección	IP 10.19.8.84, DHCP	FIGURA 14 PING PCA – PCB IPV4 

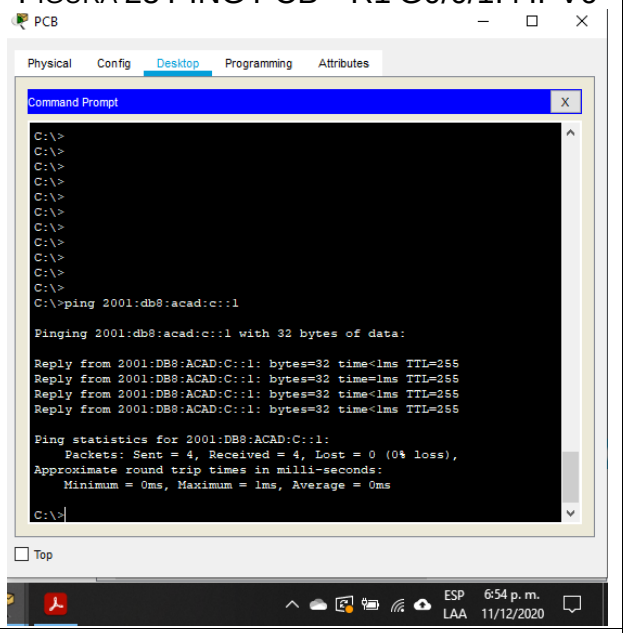
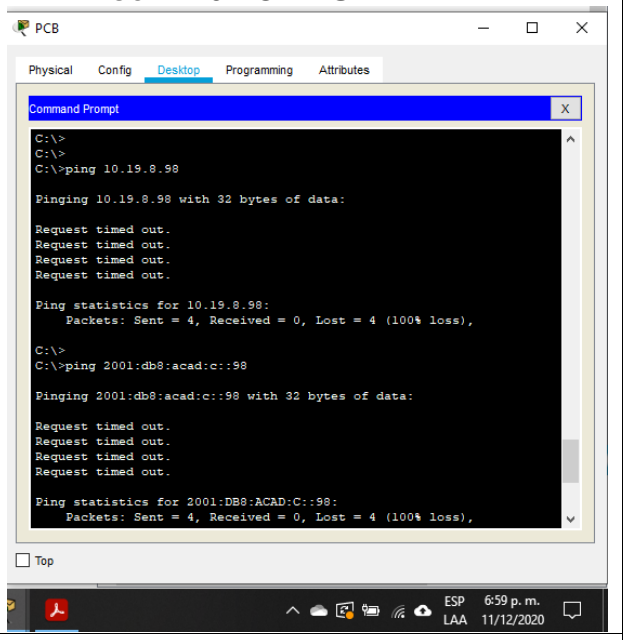
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A		IPv6	2001:db8:acad:b::50	FIGURA 15 PING PCA – PCB IPV6 
	R1 Bucle 0	Dirección	209.165.201.1	FIGURA 16 PING PCA – R1 BUCLE 0 

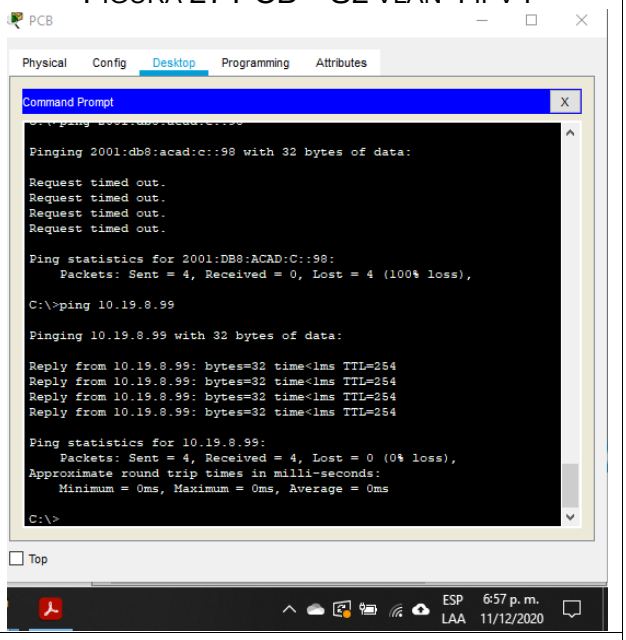
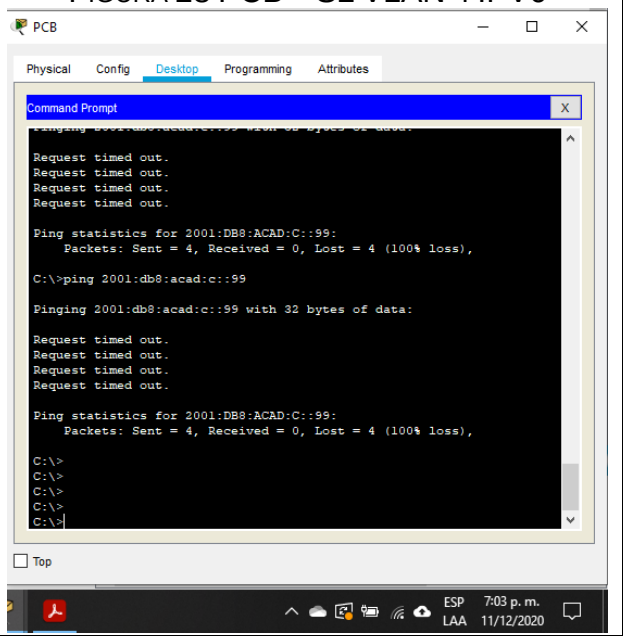
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:209: :1	FIGURA 17 PING PCA – R1 BUCLE 0 
PC-B	R1 Bucle 0	Dirección	209.165.201.1	FIGURA 18 PING PCB – R1 BUCLE0 
		IPv6	2001:db8:acad:209: :1	

Desde	A	de Internet	Dirección IP	Resultados de ping
				FIGURA 19 PING PCB – R1 BUCLE0 
	R1, G0/0/1.2	Dirección	10.19.8.1	FIGURA 20 PING PCB – R1, G0/0/1.2 IPV4 

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:a::1	**FIGURA 21** PING PCB – R1, G0/0/1.2 IPV6 
	R1, G0/0/1.3	Dirección	10.19.8.65	FIGURA 22 PING PCB – R1 G0/0/1.3 IPV4 

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b::1	FIGURA 23 PING PCB – R1 G0/0/1.3 IPV6 
	R1, G0/0/1.4	Dirección	10.19.8.97	FIGURA 24 PING PCB – R1 G0/0/1.4 IPV4 

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B		IPv6	2001:db8:acad:c::1	FIGURA 25 PING PCB – R1 G0/0/1.4 IPV6 
	S1, VLAN 4	Dirección	10.19.8.98	FIGURA 26 PCB – S1 VLAN 4 IPV4 
		IPv6	2001:db8:acad:c::98	*No Exitoso*

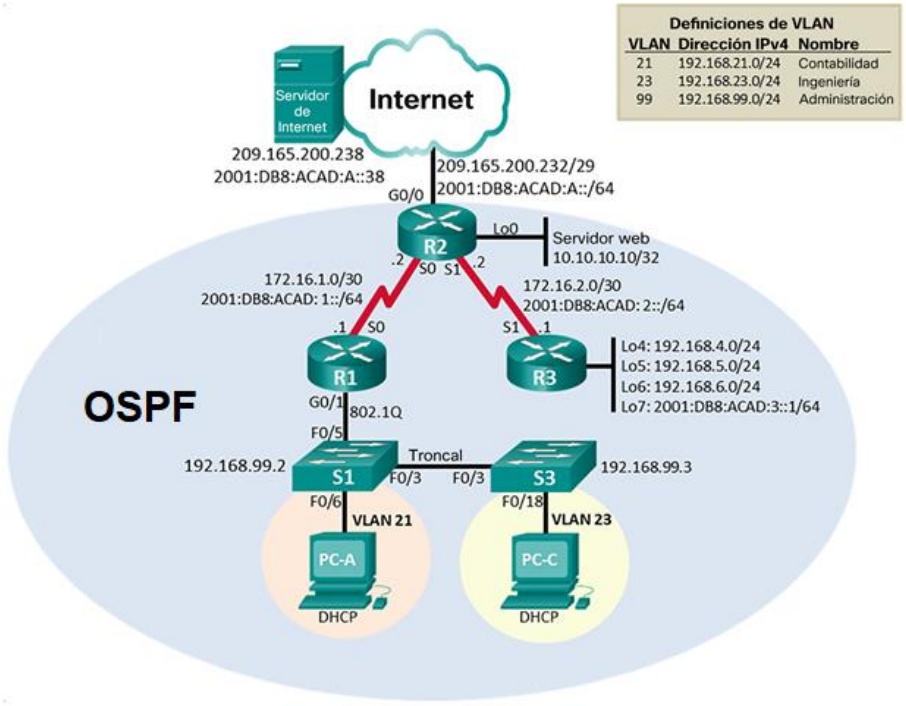
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	FIGURA 27 PCB – S2 VLAN 4 IPV4 
		IPv6	2001:db8:acad:c::99	FIGURA 28 PCB – S2 VLAN 4 IPV6 

Analizando los datos tomados desde la tabla anterior se evidencia que la red funciona correctamente y que la conectividad entre los dos equipos es verídica. En los pings no exitosos se evidencia problemas con el firewall.

2. Escenario 2.

Escenario**:** Se configura 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 29. ESCENARIO 2



2.1 Inicializando los dispositivos

2.1.1 Inicializando y volviendo a cargar los routers y los switches del escenario.

TABLA 11 INICIALIZANDO LOS DISPOSITIVOS.

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

Se realiza el borrado de las configuraciones pasadas de los equipos para que no se generen conflictos mas adelante.

2.2 Configurando los parámetros básicos de los dispositivos.

2.2.1 Configurando la computadora de Internet.

De acuerdo con la topología mostrada en la imagen del escenario 2, podemos llegar a la siguiente confirmación:

TABLA 12. CONFIGURANDO LA COMPUTADORA DE INTERNET.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233

Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

2.3 configurando los routers.

2.3.1 Configurando R1.

TABLA 13. CONFIGURANDO R1

Elemento o tarea de configuración	Especificación
Se desactiva la búsqueda DNS en el router.	Router(config)#no ip domain-lookup
Se asigna el nombre del router “R1”	R1 Router#conf t Router(config)#hostname R1 R1(config)#
Se asigna la contraseña “class” como exec privilegiado cifrada	R1(config)#enable secret class
Se configura la contraseña de acceso a la consola como “cisco”	Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#exec-timeout 4 0 R1(config-line)#login
Contraseña de acceso Telnet	cisco
Se realiza el cifrado de las contraseñas de texto no cifrado	R1(config)# service password-encryption
Se establece un MOTD que prevenga el acceso no autorizado.	R1(config)#banner motd $ SE PROHIBE EL ACCESO NO AUTORIZADO $
Se realiza la configuración de la interfaz S0/0/0 Se configura el acceso mediante IPV6 Se establece la hora en el router y se activa la interfaz.	Establezca la descripción Router(config)#interface s0/0/0 Router(config-if)#description Interfaz a R2 Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones

	Router(config)#interface s0/0/0 Router(config-if)#ip address 172.16.1.1 255.255.255.252 Router(config-if)#no shut Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Router(config)#interface s0/0/0 Router(config-if)#ipv6 address 2001:db8:acad:1::/64 Router(config-if)#no shutdown Establecer la frecuencia de reloj en 128000 Activar la interfaz Router(config)#interface s0/0/0 Router(config-if)#clock rate 128000 Router(config-if)#no shut
Se establecen las rutas de acceso predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 Router(config)#ipv6 route 0:0:0:0::0/0 s0/0/0

2.3.2 Configurando R2.

TABLA 14. CONFIGURANDO R2

Elemento o tarea de configuración	Especificación
Se desactiva la búsqueda DNS en el router.	Router(config)#no ip domain-lookup
Se asigna el nombre del router “R2”	R2 Router#conf t

	Router(config)#hostname R2 R2(config)#
Se asigna la contraseña “class” como exec privilegiado cifrada	R2(config)#enable secret class
Se configura la contraseña de acceso a la consola como “cisco”	Cisco R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#exec-timeout 4 0 R2(config-line)#login
Se asigna la contraseña de acceso Telnet	cisco
Se realiza el cifrado de las contraseñas de texto no cifrado	R2(config)# service password-encryption
Se habilita el servidor HTTP	R2(config)# ip http server R2(config)# ip http secure-server R2(config)# ip http authentication local
Se establece un MOTD que prevenga el acceso no autorizado.	R2(config)#banner motd $ SE PROHIBE EL ACCESO NO AUTORIZADO $
Se configura la interfaz S0/0/0	Establezca la descripción Router(config)#interface s0/0/0 Router(config-if)#description Interfaz a R1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Router(config)#interface s0/0/0 Router(config-if)#ip address 172.16.1.2 255.255.255.252 Router(config-if)#no shut Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Router(config)#interface s0/0/0 Router(config-if)#ipv6 address 2001:db8:acad:1::2/64 Router(config-if)#no shutdown

	Activar la interfaz
Se realiza la configuración de la Interfaz S0/0/0. Se habilita la conectividad IPV6. Se enciende la interfaz Se realiza la configuración de la Interfaz S0/0/1. Se habilita la conectividad IPV6. Se establece la hora en el router Se enciende la interfaz.	Establecer la descripción Router(config)#interface s0/0/1 Router(config-if)#description Interfaz a R3 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Router(config)#interface s0/0/0 Router(config-if)#ip address 172.16.2.2 255.255.255.252 Router(config-if)#no shut Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Router(config)#interface s0/0/1 Router(config-if)#ipv6 address 2001:db8:acad:2::2/64 Router(config-if)#no shutdown Establecer la frecuencia de reloj en 128000. Router(config-if)#clock rate 128000 Activar la interfaz Router(config-if)#no shutdown
Se realiza la configuración de la interfaz G0/0, ya que esta se usa para (simulación de Internet).	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Router(config)#interface g0/0 Router(config-if)#ip address 209.165.200.233 255.255.255.248

	Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Router(config)#interface g0/0 Router(config-if)#ipv6 address 2001:db8:acad:a::1/64 Activar la interfaz Router(config-if)#no shutdown
Se configura la interfaz loopback 0, la cual simula la conexión del servidor web.	Establecer la descripción. Router(config)#interface Loopback 0 Router(config-if)#description Servidor WEB Establezca la dirección IPv4. Router(config)#interface Loopback 0 Router(config-if)#ip address 10.10.10.10 255.255.255.255
Se configura la ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Router(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. Router(config)#ipv6 route 0:0:0:0::0/0 g0/0

2.3.3 Configurando R3

TABLA 15. CONFIGURANDO R3

Elemento o tarea de configuración	Especificación
Se desactiva la búsqueda DNS en el router.	Router(config)#no ip domain-lookup
Se asigna el nombre del router “R3”	R3 Router#conf t

	Router(config)#hostname R3 R3(config)#
Se asigna la contraseña “class” como exec privilegiado cifrada	R3(config)#enable secret class
Se configura la contraseña de acceso a la consola como “cisco”	Cisco R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#exec-timeout 4 0 R3(config-line)#login
Se asigna la contraseña de acceso Telnet	cisco
Se realiza el cifrado de las contraseñas de texto no cifrado	R3(config)# service password-encryption
Se establece un MOTD que prevenga el acceso no autorizado.	R3(config)#banner motd $ SE PROHIBE EL ACCESO NO AUTORIZADO $
Se configura la interfaz S0/0/1	
Se realiza la configuracion de la interfaz loopback 4, asignando dirección IP y Mascara de subred.	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
Se realiza la configuracion de la interfaz loopback 5, asignando dirección IP y Mascara de subred.	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
Se realiza la configuracion de la interfaz loopback 6, asignando dirección IP y Mascara de subred.	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
Se realiza la configuracion de la interfaz loopback 7, asignando dirección IP y Mascara de subred.	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface Loopback 7

	R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Se establece la configuración de las rutas predeterminadas	Configure una ruta IPv4 predeterminada de s0/0/1 Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 Configure una ruta IPv6 predeterminada de s0/0/1 Router(config)#ipv6 route 0:0:0:0::0/0 s0/0/1

2.4 Configurando los switch

2.4.1 Configurando S1.

TABLA 16 CONFIGURANDO S1

Elemento o tarea de configuración	Especificación
Se realiza la desactivación de la búsqueda de DNS	Switch(config)#no ip domain-lookup
Se asigna el nombre del switch “S1”	S1 Switch(config)#hostname S1
Se establece la contraseña de exec privilegiado cifrada como “class”.	Class
Se configura la contraseña de acceso a la consola “cisco”	Cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#exec-timeout 4 0 S1(config-line)#login
Se configura la contraseña de acceso Telnet “cisco”	cisco
Se realiza la instrucción del cifrado para las contraseñas.	S1(config)# service password-encryption
Se coloca un mensaje MOTD para evitar accesos no autorizados.	S1(config)#banner motd $ SE PROHIBE EL ACCESO NO AUTORIZADO $

2.4.2 Configurando S3.

TABLA 17. CONFIGURANDO S3

Elemento o tarea de configuración	Especificación
Se realiza la desactivación de la búsqueda de DNS	Switch(config)#no ip domain-lookup
Se asigna el nombre del switch “S3”	S3 Switch(config)#hostname S3
Se establece la contraseña de exec privilegiado cifrada como “class”.	Class S3(config)#enable secret Class
Se configura la contraseña de acceso a la consola “cisco”	Cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#exec-timeout 4 0 S3(config-line)#login
Se configura la contraseña de acceso Telnet “cisco”	cisco
Se realiza la instrucción del cifrado para las contraseñas.	S3(config)# service password-encryption
Se coloca un mensaje MOTD para evitar accesos no autorizados.	S3(config)#banner motd $ SE PROHIBE EL ACCESO NO AUTORIZADO $

2.5 Pruebas y verificación de la conectividad entre los dispositivos de red.

Se realizan utilizando el comando ping y así probar la conectividad entre dos dispositivos de la red.

TABLA 18. REALIZACIÓN DE PRUEBAS DE CONECTIVIDAD.

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

Se procede a la realización de las pruebas de conectividad mediante el comando ping en la red, se evidencian todos los casos exitosos como se muestran en las siguientes figuras.

FIGURA 30 PING DESDE R1 A R2

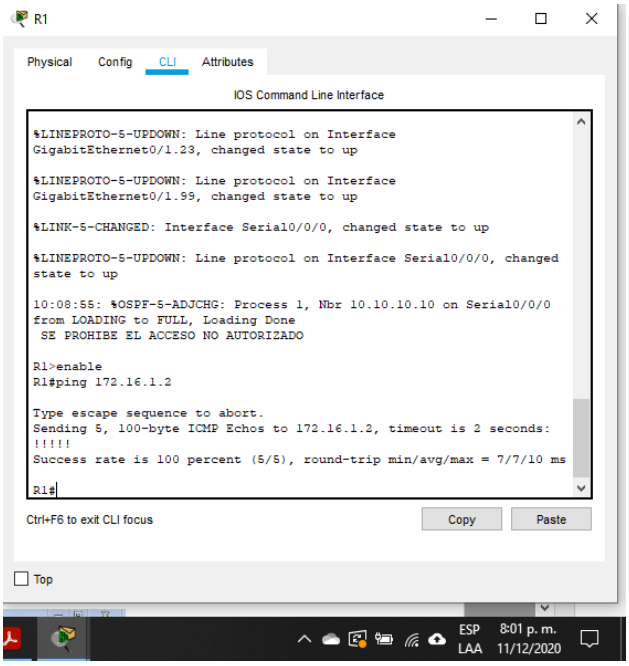


FIGURA 31 PING DESDE R2 A R3

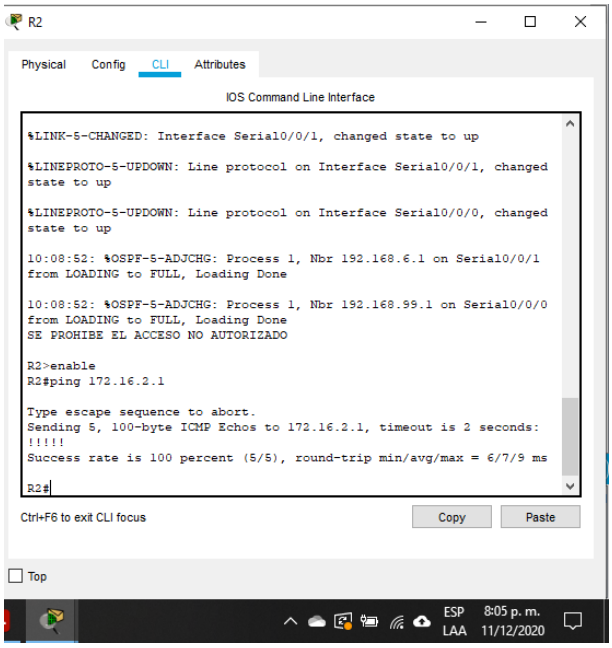
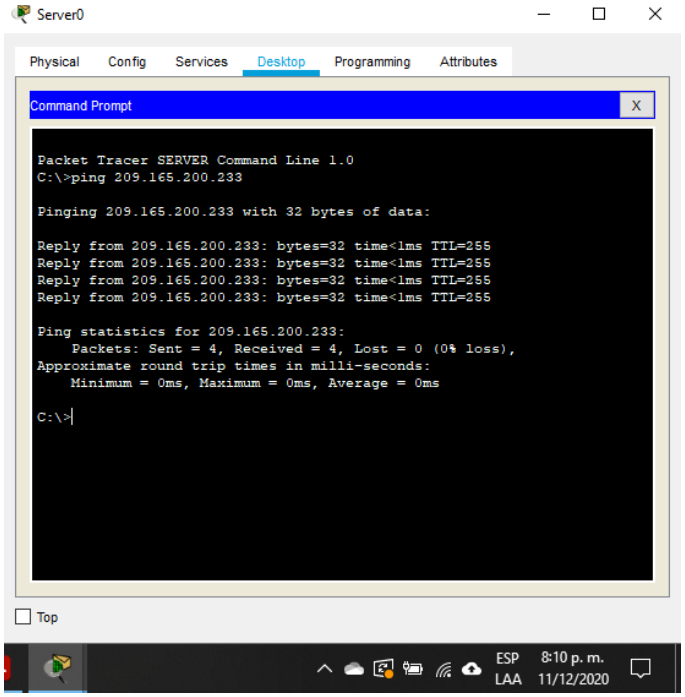


FIGURA 32 PING ENTRE PC DE INTERNET (SERVIDOR) Y GATEWAY PREDETERMINADO



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

2.6.1 Configuracion Switch 1 (S1)

TABLA 19. CONFIGURACIÓN S1.

Elemento o tarea de configuración	Especificación
Se inicia creando la base de datos de VLAN solicitadas según la topología de red.	VLAN 21, name Contabilidad VLAN 23, name Ingenieria VLAN 99, name Administracion S1(config)# vlan 21 S1(config-vlan)# name Contabilidad S1(config-vlan)# vlan 23 S1(config-vlan)# name Ingenieria S1(config-vlan)# vlan 99

	S1(config-vlan)# name Administracion S1(config-vlan)# end
Se asigna la dirección IP de administración a la VLAN 99.	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
Se asigna el gateway predeterminado.	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Se hace la configuración de la interface F0/3 para forzar el enlace troncal.	Utilizar la red VLAN 1 como VLAN nativa Interfaces F0/3 S1(config)# interface f0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1
Se hace la configuración de la interface F0/5 para forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa Interfaces F0/5 S1(config)# interface f0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1
Se realiza la configuración del resto de los puertos como puertos de acceso.	Utilizar el comando interface range Sin usar f01,2, S1(config)#interface range f0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#shutdown F0/4 S1(config)#interface f0/4

	S1(config-if)#switchport mode access S1(config-if)#shutdown F0/7-24 S1(config)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#shutdown
Se realiza la asignación de la interface F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Se apagan todos los puertos sin usar en el dispositivo.	S1(config)#interface range f0/1-2 S1(config-if-range)#shutdown F0/4 S1(config)#interface f0/4 S1(config-if)#shutdown F0/7-24 S1(config)#interface range f0/7-24 S1(config-if-range)#shutdown

2.6.2 Configuracion Switch 3 (S3)

TABLA 20. CONFIGURACIÓN S3.

Elemento o tarea de configuración	Especificación
Se inicia creando la base de datos de VLAN solicitadas según la topología de red.	VLAN 21, name Contabilidad VLAN 23, name Ingenieria VLAN 99, name Administracion S3(config)# vlan 21 S3(config-vlan)# name Contabilidad S3(config-vlan)# vlan 23

	S3(config-vlan)# name Ingenieria S3(config-vlan)# vlan 99 S3(config-vlan)# name Administracion S3(config-vlan)# end
Se asigna la dirección IP de administración a la VLAN 99.	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
Se asigna el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Se hace la configuración de la interface F0/3 para forzar el enlace troncal.	Utilizar la red VLAN 1 como VLAN nativa Interfaces F0/3 S3(config)# interface f0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1
Se realiza la configuración del resto de los puertos como puertos de acceso.	Utilizar el comando interface range Puertos sin usar F0/1-2 S3(config)#interface range f0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown F0/4-17 S3(config)#interface range f0/4-17 S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown F0/19-24 S3(config)#interface range f0/19-24

	S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown G0/1-2 S3(config)#interface range g0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#shutdown
Se realiza la asignación de la interface F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Se apagan todos los puertos sin usar en el dispositivo.	Puertos sin usar F0/1-2 S3(config)#interface range f0/1-2 S3(config-if-range)#shutdown F0/4-17 S3(config)#interface range f0/4-17 S3(config-if-range)#shutdown F0/19-24 S3(config)#interface range f0/19-24 S3(config-if-range)#shutdown G0/1-2 S3(config)#interface range g0/1-2 S3(config-if-range)#shutdown

2.6.3 Configuración R1

TABLA 21. CONFIGURACIÓN R1 VLAN.

Elemento o tarea de configuración	Especificación
Se configura 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 g0/1.21 R1(config-subif)# description LAN de Contabilidad R1(config-subif)# encapsulation dot1q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0
Se configura 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 LAN de Ingenieria R1(config-subif)# encapsulation dot1q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0
Se 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 LAN de Administracion R1(config-subif)# encapsulation dot1q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0

Se realiza la activación de la interfaz G0/1.	R1(config)# interface g0/1

2.6.4 Verificación de la conectividad de red entre los switch y R1.

TABLA 22. VERIFICACIÓN DE LA CONECTIVIDAD DE RED ENTRE LOS SWITCH Y R1.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.3	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	No Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	No Exitoso

En la anterior *tabla 22* se evidencia que los comando ping realizados son exitosos y con algunos fallos, a continuación, se muestra las figuras.

FIGURA 33 PING DESDE S1 A R1 VLAN 99

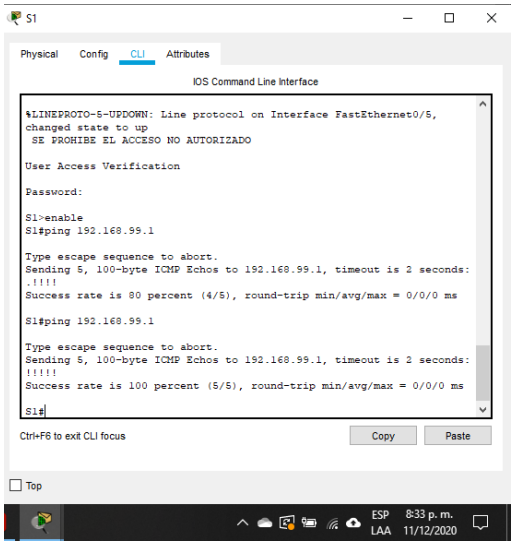


FIGURA 34 PING DESDE S3 A R1 VLAN 99

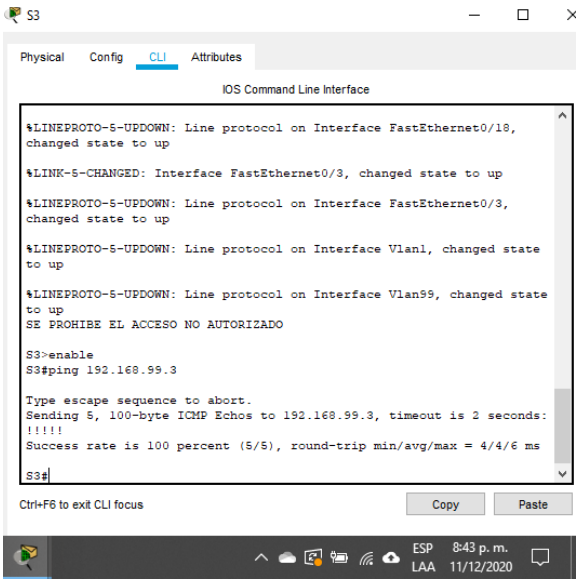


FIGURA 35 PING DESDE S1 A R1 VLAN 21

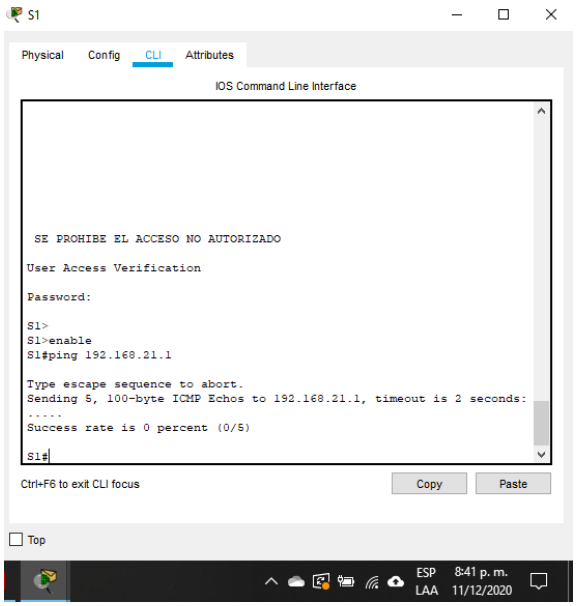
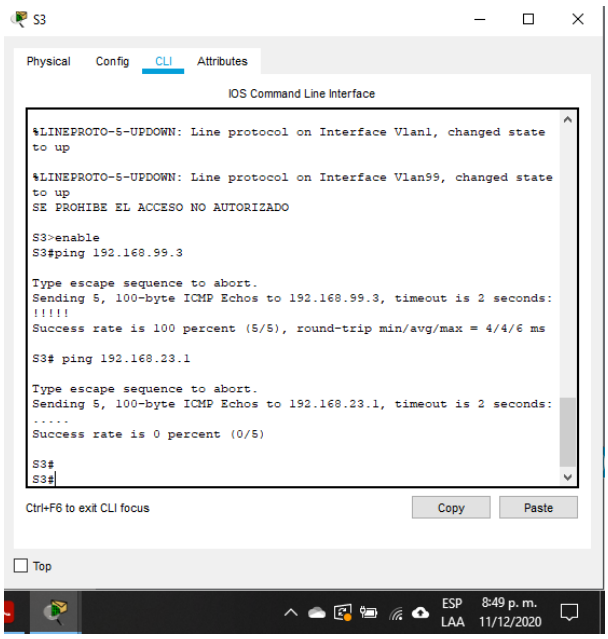


FIGURA 36 PING DESDE S3 A R1 VLAN 23



2.7 Configuración OSPF.

2.7.1 Configuración OSPF en el R1

TABLA 23. CONFIGURACIÓN OSPF EN EL R1

Elemento o tarea de configuración	Especificación
Se realiza la configuracion OSPF área 0 en R1	R1(config)#router ospf 1
Se Anuncian 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

Se establecen todas las interfaces LAN como pasivas	R1#conf t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#router ospf 1 R1(config-router)#passive-interface g0/1
Se realiza la desactivacion la sumarización automática, permitiendo la disminución de entradas de las actualizaciones de enrutamiento.	No aplica ya que OSPF no realiza sumarización

2.7.2 Configurar OSPF en el R2.

TABLA 24 CONFIGURACIÓN DE OSPF EN R2

Elemento o tarea de configuración	Especificación
Se realiza la configuracion OSPF área 0 en R2	R2(config)#router ospf 1
Se Anuncian 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 172.16.2.0 0.0.0.3 area 0
Se establece la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 1 R2(config-router)#passive-interface Loopback0
Se realice la desactivación de la sumarización automática.	No aplica ya que OSPF no realiza sumarización

2.7.3 Configurar OSPF en el R3.

TABLA 25 CONFIGURACIÓN DE OSPF EN R3

Elemento o tarea de configuración	Especificación
Se realiza la configuracion OSPF área 0 en R2	R3(config)#router ospf 3
Se Anuncian las redes conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.255 area 0
Se establece la interfaz LAN IPV4 (loopback) como pasivas	R3(config-router)#passiveinterface loopback 4 R3(config-router)#passiveinterface loopback 5 R3(config-router)#passiveinterface loopback 6
Se realice la desactivación de la sumarización automática.	R3(config-router)#no autosummary

2.8 Verificar la información de OSPF.

Los siguientes son comandos CLI adecuados para obtener cierta información que es de gran utilidad.

TABLA 26 COMANDOS CLI PARA OBTENER 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 protocols R2#show ip protocols R3#show ip protocols R1#show ip route R2#show ip route R3#show ip route R1#show ip ospf interface g0/1

	R2#show ip ospf interface g0/3 R3#show ip ospf interface Loopback4 R3#show ip ospf interface Loopback5 R3#show ip ospf interface Loopback6 R3#show ip ospf interface Loopback7
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show ip protocols R2#show ip protocols R3#show ip protocols

2.9 Implementar DHCP y NAT para IPv4.

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

TABLA 27 CONFIGURACIÓN DE R1 COMO SERVIDOR DHCP.

Elemento o tarea de configuración	Especificación
Se reservan las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Red 192.168.21.0 / 24 Rango hosts 192.168.21.1 - 192.168.21.254 Broadcast 192.168.21.255 EXCLUDE 192.168.21.1 - 192.168.21.19 DHCP POOL INICIAL 192.168.21.20 DHCP POOL FINAL 192.168.21.254 GATEWAY 192.168.21.1 Mask 255.255.255.0
Se reservan las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Red 192.168.23.0 / 24 Rango hosts 192.168.23.1 - 192.168.23.254 Broadcast 192.168.23.255

	EXCLUDE 192.168.23.1 - 192.168.23.19 DHCP POOL INICIAL 192.168.23.20 DHCP POOL FINAL 192.168.23.254 GATEWAY 192.168.23.1 Mask 255.255.255.0
Se crea 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 excluded-address 192.168.21.1 192.168.21.19 R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#domain-name ccna-sa.com R1(config)#ip name-server 10.10.10.10
Se crea 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 excluded-address 192.168.23.1 192.168.23.19 R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#domain-name ccna-sa.com R1(config)#ip name-server 10.10.10.10

2.10 configuración de la NAT estática y dinámica en el R2.

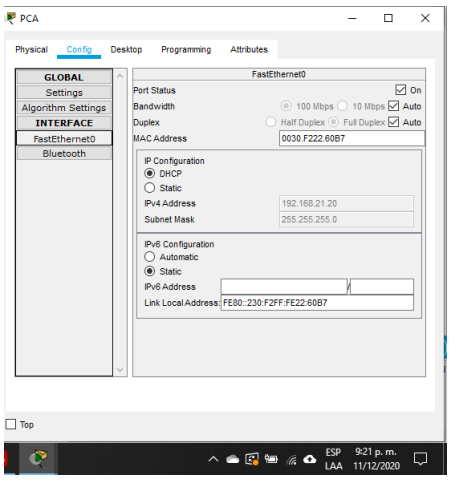
TABLA 28 CONFIGURACIÓN DE LA NAT ESTÁTICA Y DINÁMICA EN EL R2

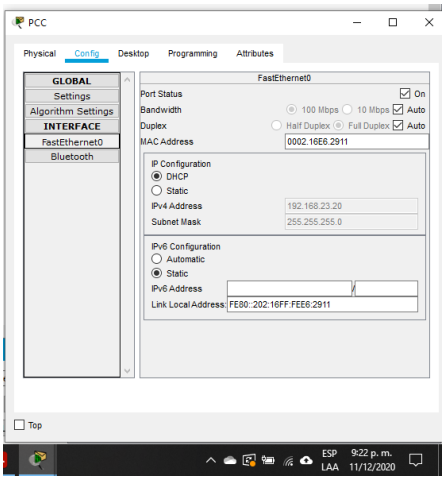
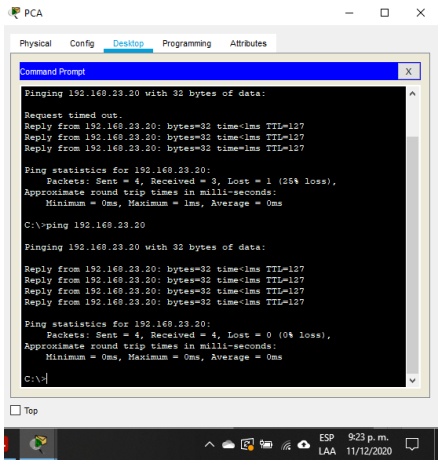
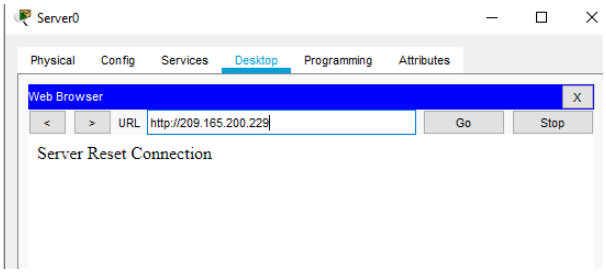
Elemento o tarea de configuración	Especificación
Se crea una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15 R2(config)# username webuser privilege 15 secret cisco12345
Se habilita el servicio del servidor HTTP	R2(config)# ip http server
Se configura el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)# ip http authentication local
Se crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229 R2(config)# ip route 10.10.10.10 255.255.255.255 209.165.200.229 R2(config)# ip nat inside source static 10.10.10.10 209.165.200.229
Se realiza la asignación a la interfaz interna y externa para la NAT estática	R2(config)# interface Loopback0 R2(config-if)# ip nat inside R2(config-if)# interface g0/0 R2(config-if)# ip nat outside
Se configura 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 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
Se establece y define 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 255.255.255.248
Se define la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET

2.11 Verificar el protocolo DHCP y la NAT estática.

TABLA 29 VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	FIGURA 37 INFRMACION DHCP EN PCA 

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	FIGURA 38 INFORMACION DHCP EN 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 39 PING ENTRE PCA Y PC C 
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	FIGURA 40 ACCEDIENDO AL SERVIDOR WEB  No es posible realizar este evento en el packet tracer.

2.12 Configurar NTP.

TABLA 30 CONFIGURACIÓN NTP

Elemento o tarea de configuración	Especificación
Se realiza el ajuste la fecha y hora en R2.	5 de marzo de 2016, 9 a. m. R2#show clock detai R2# clock set 9:00:00 5 March 2016
Se configura R2 como un maestro NTP.	Nivel de estrato: 5 R2#conf t R2(config)# ntp master 5
Se configura R1 como un cliente NTP.	Servidor: R2 R1(config)# ntp server 172.16.1.2
Se configura R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)# ntp update-calendar
Se verifica la configuración de NTP en R1.	R1# show ntp status | include Clock

2.13 Listas de control de acceso (ACL)

2.13.1 restringir el acceso a las líneas VTY en el R2

TABLA 31 RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Elemento o tarea de configuración	Especificación
Se configura una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2#conf t R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1

	R2(config-std-nacl)#exit
Se aplica 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
Se realiza la verificacion que la ACL funcione como se espera	

FIGURA 41 PRUEBA ACL 1

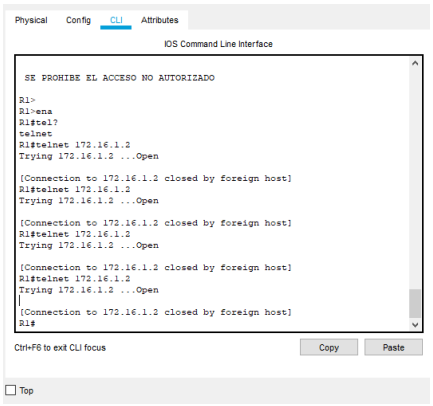
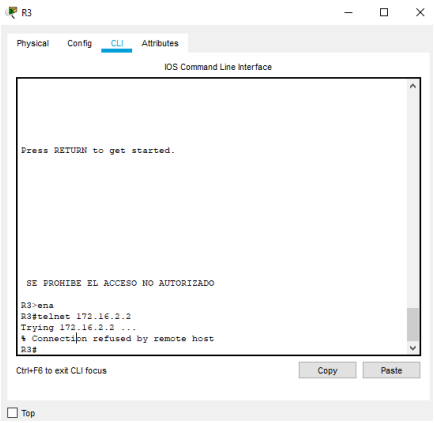
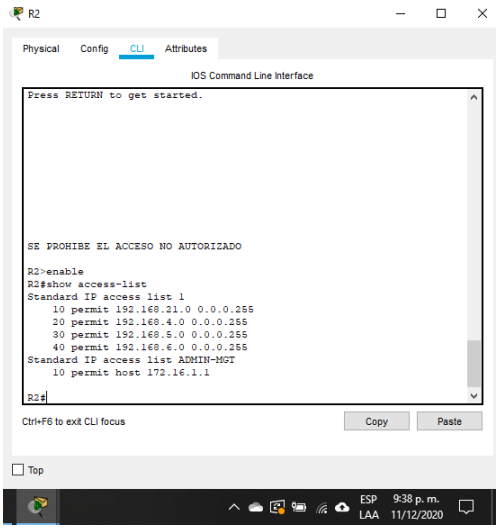
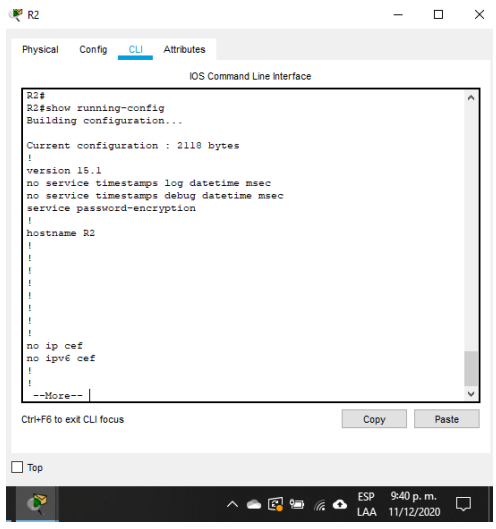


FIGURA 42 PRUEBA ACL 2



2.13.2 Introducir comando CLI para mostrar información necesaria.

TABLA 32 COMANDOS CLI PARA ACL

Descripción del comando	Entrada del estudiante (comando)
Se Muestrn las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists ADMIN-MGT FIGURA 43 CONCIDENCIAS LISTA DE ACCESO 
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show running-config FIGURA 44 MOSTRANDO ACL 

¿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. R2# show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2# clear ip nat translation * R2# clear ip nat statistics

CONCLUSIONES

En el escenario 1, se colocaron a prueba los conocimientos adquiridos mediante el análisis de diversos protocolos y métricas de enrutamiento.

En el escenario 1 se evidencio la necesidad de que los swictch de packet tracer traen una ios con versión 12 la cual no permite ipv6 , se realizó una actualización mediante una conexión a un servidor para quedar a la versión 15.

En ambos escenarios, se realizaron diversas pruebas que permiten evidenciar el funcionamiento correcto de las redes creadas para los escenarios propuestos.

En ambos escenarios se tuvo la oportunidad de aplicar el conocimiento adquirido en el diplomado de profundización en el desarrollo de esta prueba de habilidades practica final.

BIBLIOGRAFIA

Di Tommaso, L. (28 de Febrero de 2010). CONFIGURACIÓN DE PPP Y PAP EN CISCO. Obtenido de https://www.mikroways.net/2010/02/28/configuracion-de-ppp-y-pap-en-cisco/

Martinez G., V. E. (20 de Febrero de 2013). Configuración de rutas estáticas (static route) Router Cisco. Obtenido de http://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route-router-cisco/

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. recuperado de https://static-course assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1. (s.f.).

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1. (s.f.).

W0LF_F4NG, 2020. Configuración Básica Ipv6 Router Cisco. [online] WFNetworking. Recuperado de: https://www.w0lff4ng.org/configuracion-basicaipv6-router-cisco/

ANEXOS

ANEXO 1

(Enlace de descarga de los archivos de simulación escenario 1 y 2)
https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/jjramirezlon_unadvirtual_edu_co/Es8mubD1QNJIgc9iVcATrEgBibM3yxgcvR-VLNclHqYoEQ?e=wicpRs

ANEXO 2

(Enlace de descarga para el Articulo Científico IEEE)
https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/jjramirezlon_unadvirtual_edu_co/Es8mubD1QNJIgc9iVcATrEgBibM3yxgcvR-VLNclHqYoEQ?e=wicpRs