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

CESAR VILLAMIL RUIZ

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

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

CESAR VILLAMIL RUIZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO SISTEMAS

DIRECTOR: DIEGO EDINSON RAMIREZ CLAROS

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

FACATATIVA, 30 de noviembre de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

MODELO OSI
Este es un modelo que sirve como estándar de referencia que fija los modelos de las comunicaciones; inicialmente fue creado por la ISO y actualmente se mantiene ya que permite estandarizar la comunicación global de internet y también de área local por medio del establecimiento de protocolos de comunicación entre equipos de cómputo, en este sentido todos los paquetes enviados atraviesan las 7 capas de este modelo OSI.

PROTOCOLO DE RED
Es el conjunto de reglas estándar que se utilizan para la comunicación en redes de computadores de cualquier tipo, ya sean LAN, WAN, etc. Por los que se establece una semántica y sintaxis a seguir para que sea más fácil de entender a la misma vez que funciona de la manera más optima.

RED DE ÁREA AMPLIA (WAN):
Es el conjunto de redes más pequeñas que cubren gran parte del planeta por lo que permiten la comunicación hoy en día entre usuarios de distintos lugares comunicarse casi en tiempo real incluso a miles de kilómetros de distancia dando una gran velocidad que cada vez se ha ido aumentando en capacidad ya que la demanda mundial del servicio es muy grande, en este caso se hacen conexiones de todo tipo cableadas, inalámbricas y satelitales para poder brindar servicios de conexión a tantos usuarios.

RED DE ÁREA LOCAL (LAN):
Se define como un conjunto de dispositivos conectados en una red local, en donde estos dispositivos de cómputo o móviles pueden compartir información como archivos, documentos y datos, es decir, entre ellos puede haber envió de estos archivos, un ejemplo es cuando en alguna oficina todos los computadores están conectados. En este caso los dispositivos se pueden conectar a la red por medios cableados o inalámbricos.

RESUMEN

Se ha realizado el desarrollo de los dos escenarios de la prueba de conocimientos y habilidades donde se configuro una red utilizando el simulador Packet Tracer, esta red está compuesta por cinco dispositivos los cuales se comunican en una red de área local LAN y otra red WAN utilizando configuración de direccionamiento Ipv4 e Ipv6 en algunos casos estática y en otros casos dinámica; además la configuración de los dispositivos (switch y routers) se realizó desde cero ya que se ha aplicado una buena práctica la cual es elemental y consiste en elimina la configuración inicial de los dispositivos para configurarlos totalmente desde cero. Por último, como prueba del correcto funcionamiento se hace conexión entre todos los dispositivos por medio del comando ping que se ejecuta siempre desde la consola de comandos de las computadoras y permite evidenciar de manera precisa si hay o no conexión.

Palabras Clave: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

ABSTRACT

The development of the two scenarios of the knowledge and skills test has been carried out where a network was configured using the Packet Tracer simulator, this network is composed of five devices which communicate in a LAN local area network and another WAN network using configuration of IPv4 and IPv6 addressing in some cases static and in other cases dynamic; In addition, the configuration of the devices (switches and routers) was made from scratch since a good practice has been applied which is elementary and consists of eliminating the initial configuration of the devices to configure them completely from scratch. Finally, as proof of correct operation, a connection is made between all the devices by means of the ping command that is always executed from the computers command console and allows to show precisely whether or not there is a connection.

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

INTRODUCCIÓN

Desde los orígenes más antiguos de la humanidad la comunicación ha sido muy importante y al pasar de los años se han desarrollado de manera cada vez más acelerada; teniendo en cuenta que desde el siglo pasado y en especial con fines militares se ha evolucionado todo lo referente a las telecomunicaciones; también se evidencia el gran avance en protocolos de comunicación pasando por los aspectos referentes tanto a hardware y software cada vez más eficientes.

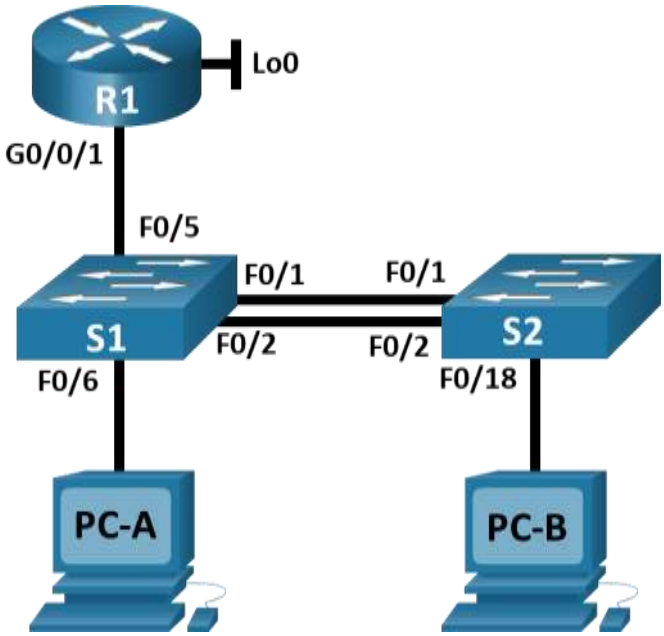
Actualmente se utilizan gran variedad de medios para transmitir información entre los más comunes se encuentran el microondas, satelital, ondas electromagnéticas, o por fibras de vidrio, y todos estos aplican el modelo OSI como estándar para la transmisión de datos entre dispositivos.

En este caso se ha configurado una red LAN y otra WAN por medio del direccionamiento Ipv4 e Ipv6 en los computadores como en los switch y router. Además, se han creado las correspondientes Vlans, para garantizar la comunicación entre equipos por medio de los switch y se restringió el ingreso a configuración tanto de switch como de router usando contraseñas en línea de consola y acceso al modo privilegiado de configuración.

DESARROLLO

1 ESCENARIO 1

Figura 1. ESCENARIO 1



1.1 CONFIGURACIÓN INICIAL

Se eligen los siguientes componentes físicos en el packet tracer teniendo siempre en cuenta la topología y las funcionalidades de cada dispositivo, ya que en este caso que se va a trabajar con la configuración de IPv6; se tiene que utilizar dispositivos que permitan esta configuración:

- Router 4321 (R1)
- Switch 3650 (S1)
- Switch 3650 (S2)
- Computador de escritorio (PC-A)
- Computador de escritorio (PC-B)

En este caso se utiliza el Switch 3650 dado el caso de que en el simulador packet tracer si permite configurar direcciones IPV6.

En este caso se hace el cableado de la siguiente manera donde únicamente se utilizó cable directo:

Tabla 1. Cableado

Tipo de cable	Punto de origen	Punto Destino
Cable directo	R1 g0/0/1	S1 g1/0/5
Cable directo	S1 g1/0/5	PC-A f0
Cable directo	S2 g1/0/18	PC-B f0
Cable directo	S1 g1/0/1	S2 g1/0/1
Cable directo	S1 g1/0/2	S2 g1/0/2

Figura 2. Escenario 1 Simulación

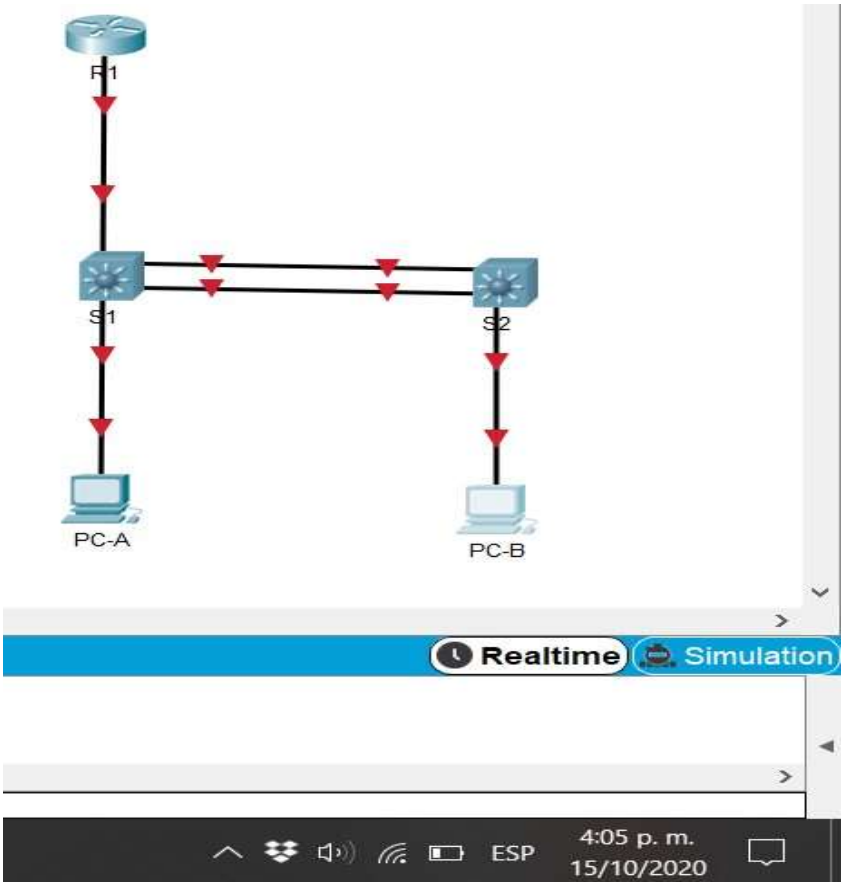


Tabla 2. VLAN

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

Esta tabla muestra las 5 Vlan que se van a configurar y utilizar en la red.

1.2 CONFIGURACIÓN DE DIRECCIONAMIENTO IP EN LA TOPOLOGIA

En este caso se lleva a cabo la siguiente configuración de direcciones tanto IPV4 como IPV6 según la topología.

La tabla a continuación es demasiado importante ya que permite tener claro que direcciones tanto Ipv4 como Ipv6 en cada dispositivo; esta tabla siempre se debe hacer antes de empezar a configurar los dispositivos y se hace teniendo en cuenta los requerimientos de la topología.

Tabla 3. Direccionamiento IP

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
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
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
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
	2001:db8:acad:b: :50 /64	fe80::1

Esta tabla muestra el direccionamiento Ip y en que interfaz del dispositivo se debe configurar.

Inicialmente se empieza borrando la configuración inicial del router y switch en la topología.

Seguidamente se conecta el PC-A desde el puerto de consola hacia el puerto de consola de R1 por medio de cable de consola, que es como se haría en la vida real y elimina la configuración inicial de R1 mediante los siguientes comandos:

Tabla 4. Borrar parámetros de la NVRAN en router

Tarea	Especificación
Entrar al modo privilegiado	Router>enable
Borrar la memoria NVRAM	Router#erase startup-config
Recargar el dispositivo nuevamente	Router#reload

Seguidamente se procede a coloca la fuente de poder en el S1 y se conecta por Cable de consola desde el mismo puerto de consola hacia el PC-B. Ya estando conectados se ingresa desde el terminal del PC-b para configurar
S1 mediante los siguientes comandos:

Tabla 5. Borrado de configuración fabrica en siwtch

Tarea	Especificación
Entrar al modo privilegiado	Switch>enable
Borrar la configuración inicial	Switch#erase startup-config Switch#delete vlan.dat
Recargar el dispositivo nuevamente	Switch#reload

Luego se hace el mismo procedimiento con S2 por lo que hay necesidad de conectar la fuente de poder y se conecta desde puerto de consola de PC-B hacia el puerto de consola de S2, y ejecutar los mismos comandos.

1.3 VERIFICACIÓN PARA SABER SI LOS SWITCH SOPORTAN IPV6

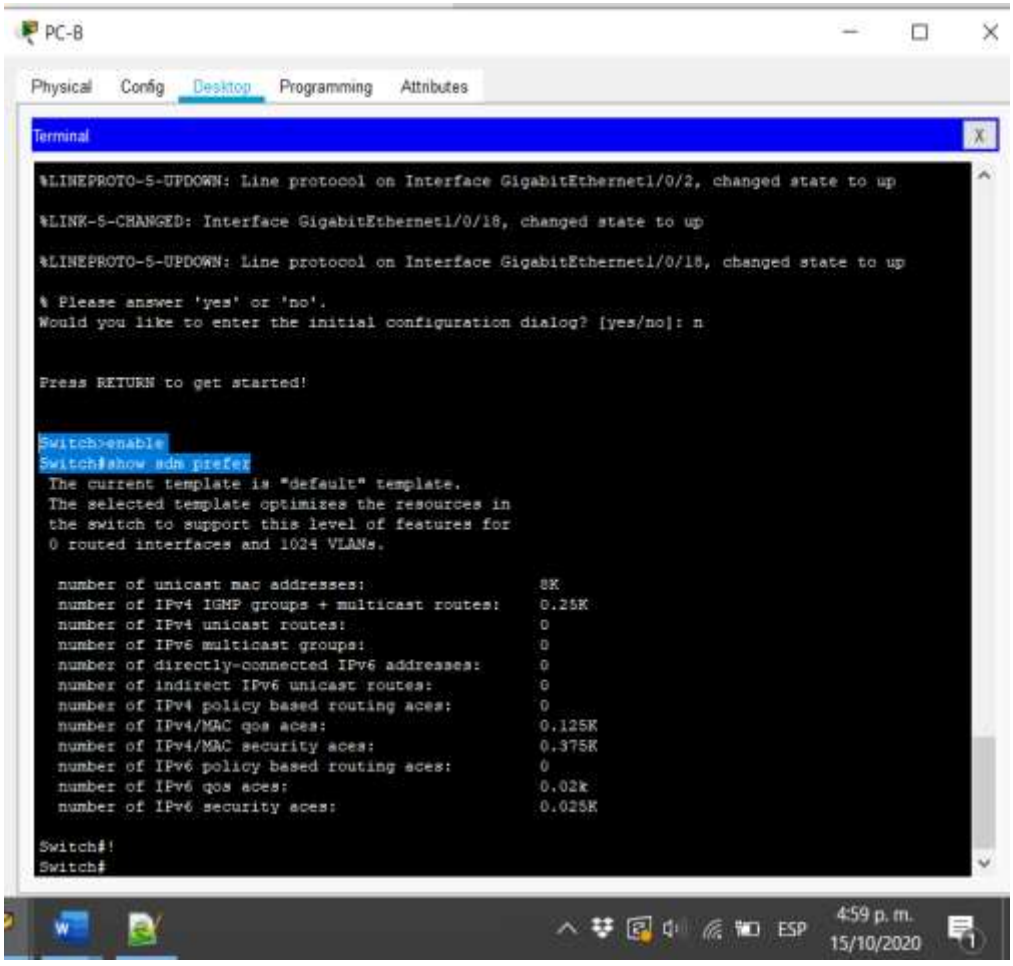
Se ejecutan el siguiente comando desde el PC-B conectado por medio de la consola con S1:

Tabla 6. Verificación de funcionamiento con Ipv6 en switch

Tarea	Especificación
Verificar si el dispositivo soporta direccionamiento IPV6	Switch>enable Switch#show sdm prefer

Se ejecutan el comando Show sdm prefer desde el PC-B conectado por medio de la consola con S2 para saber si S2 permite la configuración de Ipv6.

Figura 3. Comprobación Switch Con Ipv6



En este caso se evidencia que los dos switch admiten IPV6.

1.4 CONFIGURACIÓN DE R1

Esta configuración se hace desde el PC-A conectado por medio de cable de consola hacia R1.

Inicialmente lo que se hace es configurar lo más básico como las contraseñas para proteger el dispositivo por medio de la petición de contraseñas y el cifrado de las mismas; también se debe habilitar el ruteo por Ipv6.

Luego se configuran las direcciones Ipv4 e Ipv6 correspondientes a cada interfaz que se va a utilizar del dispositivo.

Tabla 7. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain lookup Router(config)#
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	R1(config-line)#exit R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes 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)#ipv6 address fe80::1 link-local R1(config-subif)#int g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes 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)#int g0/0/1.4 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)#ipv6 address fe80::1 link-local R1(config-subif)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown

Tarea	Especificación
Configure el Loopback0 interface	R1(config-if)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#description Internet
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Esta tabla muestra la configuración inicial en el router R1 para proteger y dar seguridad mediante la creación de contraseñas tanto para el ingreso al modo privilegiado como para el modo de configuración y además deben ir cifradas para mayor seguridad; también se configura las interfaces correspondientes a cada Vlan.

1.5 CONFIGURACIÓN DE S1

Inicialmente lo que se hace es configurar lo más básico como las contraseñas para proteger el dispositivo por medio de la petición de contraseñas y el cifrado de las mismas; también se debe habilitar el ruteo por Ipv6. Luego se configuran las direcciones Ipv4 e Ipv6 correspondientes a cada interfaz que se va a utilizar del dispositivo.

Tabla 8. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config-line)#exit S1(config)#username admin secret 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
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#exit S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S1(config)#int vlan 4 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)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97

Esta tabla muestra la configuración inicial en el switch S1 para proteger y dar seguridad mediante la creación de contraseñas tanto para el ingreso al modo privilegiado como para el modo de configuración y además deben ir cifradas para mayor seguridad; también se configura las interfaces correspondientes a cada Vlan.

1.6 CONFIGURACIÓN S2

Inicialmente lo que se hace es configurar lo más básico como las contraseñas para proteger el dispositivo por medio de la petición de contraseñas y el cifrado de las mismas; también se debe habilitar el ruteo por Ipv6.

Luego se configuran las direcciones Ipv4 e Ipv6 correspondientes a cada interfaz que se va a utilizar del dispositivo.

Tabla 9. Configuración S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd (Acceso no autorizado! (
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI)	S2(config)#int vlan 4S2(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)#description Management Interface S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

Esta tabla muestra la configuración inicial en el switch S2 para proteger y dar seguridad mediante la creación de contraseñas tanto para el ingreso al modo privilegiado como para el modo de configuración y además deben ir cifradas para mayor seguridad; también se configura las interfaces correspondientes a cada Vlan.

1.7 CONFIGURACIÓN DE VLAN E INTERFACES EN S1

Se empieza a configuran las Vlan, las cuales permiten comunicar a los dispositivos según las direcciones Ip en la Vlan que este habilitado, es decir, el mismo dispositivo bien sea un router o un switch puede tener diferentes Vlans y los dispositivos habilitados a una misma vlan se pueden comunicar entre sí, pero no con otros dispositivos de otras Vlan.

Tabla 10. Configuración Vlan en S1

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

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interface g1/0/5 S1(config)#int g1/0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 Interface g1/0/1 y g1/0/2 S1(config)#int range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	Interface g1/0/6 S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown

Esta tabla muestra la configuración final en el switch S1 asignando las correspondientes interfaces y deshabilitando las que no se van a utilizar.

1.8 CONFIGURACIÓN DE VLAN E INTERFACES EN S2

Se cambia el cable de consola del PC-B hacia eS2 y luego se empieza a configuran las Vlan , las cuales permiten comunicar a los dispositivos según las direcciones Ip en la Vlan que este habilitado, es decir, el mismo dispositivo bien sea un router o un switch puede tener diferentes Vlans y los dispositivos habilitados a una misma vlan se pueden comunicar entre sí, pero no con otros dispositivos de otras Vlan.

Tabla 11. Configuración Vlan en S2

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes S2>enable S2#configure terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes VLAN 3, name Trikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes VLAN 4, name Management S2(config-vlan)#vlan 4 S2(config-vlan)#name Management VLAN 5, nombre Parking S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking VLAN 6, nombre Native S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit

Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces g1/0/1 y g1/0/2 S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso del host para la VLAN 3	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if-range)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config-if-range)#int range g1/1/1-4 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown

Esta tabla muestra la configuración final en el switch S1 asignando las correspondientes interfaces teniendo en cuenta el rango de interfaces para cada Vlan y deshabilitando las que no se van a utilizar.

1.9 ACTIVACIÓN DE PUERTOS PARA CONEXIÓN ENTRE LOS DOS SWITCH

Teniendo en cuenta que por el momento se tiene la conexión de puertos G1/0/1 y G1/0/2 apagados en S1 y S2, lo que se hace es encenderlos mediante los comandos int range g1/0/1-2 seguido de no shutdown el cual enciende estas interfaces

Se realiza el mismo procedimiento de seleccionar las interfaces y encenderlas, solo conectando S1 al PC-B mediante cable de consola.

1.10 CONFIGURACIÓN DIRECCIONES EN R1

Inicialmente se conecta el PC-A hacia R1 por medio de cable de consola para proceder con la configuración

Tabla 12. Configuración de direccionamiento en R1

Tarea	Especificación
Configure Default Routing	Rutas predeterminadas para IPv4 R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 Rutas predeterminadas IPv6 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	Se crea un grupo DHCP para VLAN 2 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes 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 Se asigna el nombre correspondiente de dominio ccna-a.net R1(dhcp-config)# domain-name ccna-a.net Se configura la puerta de enlace predeterminada

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	Se crea el grupo de direcciones par el grupo DHCP para VLAN 3 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool VLAN3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 Se asigne el nombre de dominio correspondiente ccna-b.net R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Esta tabla muestra la configuración para el direccionamiento Ipv4 dinámico con el protocolo DHCP en las redes Vlan 2 y 3.

1.11 CONFIGURACIÓN DEL DIRECCIONAMIENTO DE RED EN PC-A

Para esto se debe de ir al Desktop/IP configuración y en Ipv6 configuración seleccionar Auto Config por lo cual el PC-A tomara la configuración establecida a la interfaz que está conectado.

Tabla 13. Configuración PC-A

PC-A Network Configuración	
Descripción	ccna-a.net
Dirección física	0090.2194.127D
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Esta tabla muestra la configuración de red definida para el computador PC-A.

1.12 CONFIGURACIÓN DEL DIRECCIONAMIENTO DE RED EN PC-B

Para esto se debe de ir al Desktop/IP configuración y en Ipv6 configuración seleccionar Auto Config por lo cual el PC-A tomara la configuración establecida a la interfaz que está conectado.

Tabla 14. Configuración PC-B

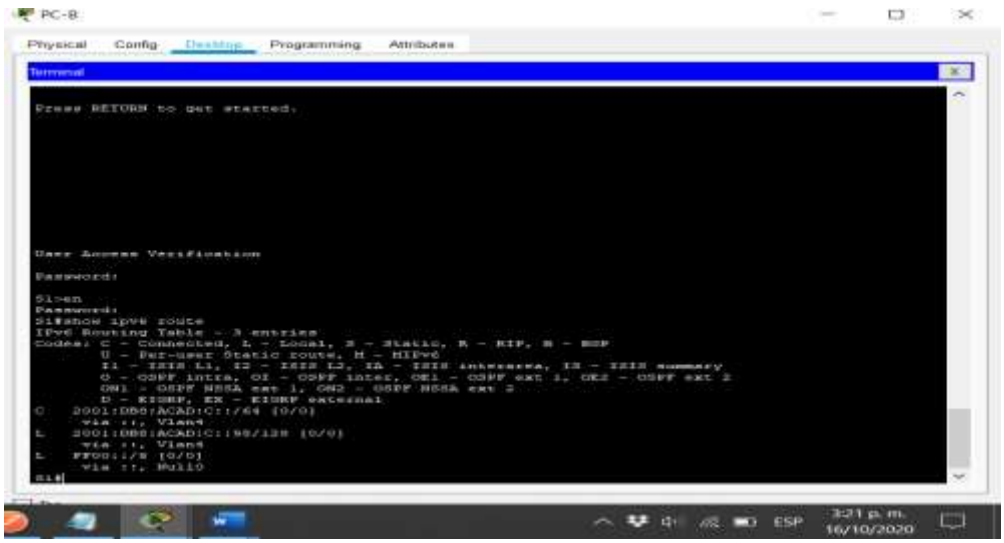
PC-B Network Configuración	
Descripción	ccna-b.net
Dirección física	0002.1687.2604
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Esta tabla muestra la configuración de red definida para el computador PC-B.

1.13 VERIFICACIÓN PUERTA DE ENLACE IPV6 EN S1

En este momento S1 no tiene habilitada la puerta de enlace para direccionamiento Ipv6, eso lo podemos comprobar mediante el comando Show ipv6 route.

Figura 4. Comprobación Puerta De Enlace Ipv6 En S1

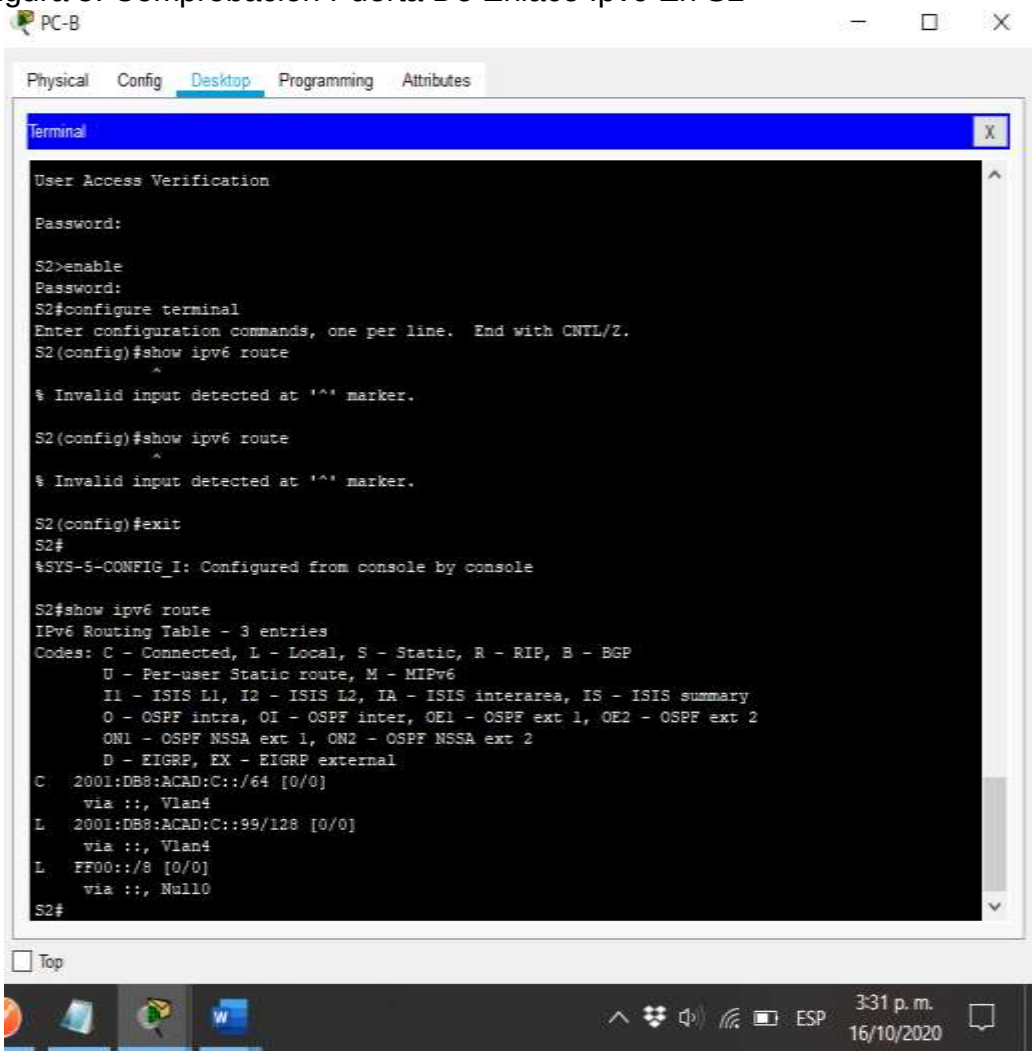


Se conecta desde PC-B hacia S1 luego se ingresa al modo de configuración con el comando configure terminal seguido de el comando ipv6 route ::/0 2001:db8:acad:c::1 para poder trabajar Ipv6 en S1.

1.14 VERIFICACIÓN PUERTA DE ENLACE IPV6 EN S2

En este momento S2 no tiene habilitada la puerta de enlace para direccionamiento Ipv6, eso lo podemos comprobar mediante el comando Show ipv6 route.

Figura 5. Comprobación Puerta De Enlace Ipv6 En S2



Se conecta PC-B hacia S2 por medio de cable de consola y se ingresa al modo de configuración con el comando configure terminal luego se ejecuta el comando ipv6 route ::/0 2001:db8:acad:c::1 para poder trabajar con Ipv6 en S2.

1.15 VERIFICACIÓN DE RED

Se procede a hacer las correspondientes pruebas de conexión mediante el comando Ping entre los diferentes dispositivos y redes, en caso de que alguno no funciones se deberá proceder a ajustar porque demuestra que alguna configuración no es la adecuada.

Tabla 15. Test de conexión en la red

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Comando: C:\>ping 10.19.8.1 Resultado: Reply from 10.19.8.1: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:a: :1	Comando: C:\>ping 2001:db8:acad:a::1 Resultado: Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.
	R1, G0/0/1.3	Dirección	10.19.8.65	Comando: C:\>ping 10.19.8.65 Resultado: Reply from 10.19.8.65: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:b: :1	Comando: C:\>ping 2001:db8:acad:b::1 Resultado: Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.
	R1, G0/0/1.4	Dirección	10.19.8.97	Comando: C:\>ping 10.19.8.97 Resultado: Reply from 10.19.8.97: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:c: :1	Comando: C:\>ping 2001:db8:acad:c::1 Resultado: Reply from 2001:DB8:ACAD:C::1: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
	S1, VLAN 4	Dirección	10.19.8.98	Comando: C:\>ping 10.19.8.98 Resultado: Reply from 10.19.8.98: bytes=32 time=6ms TTL=254 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:c::98	Comando: C:\>ping 2001:db8:acad:c::98 Resultado: Reply from 2001:DB8:ACAD:C::98: bytes=32 time<1ms TTL=254 Resultado exitoso, si hay conexión.
	S2, VLAN 4	Dirección	10.19.8.99.	Comando: C:\>ping 10.19.8.99 Resultado: Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c::99	Comando: C:\>ping 2001:db8:acad:c::99 Resultado: Reply from 2001:DB8:ACAD:C::99: bytes=32 time=1ms TTL=254 Resultado exitoso, si hay conexión.
	PC-B	Dirección	IP address will vary. 10.19.8.85	Comando: C:\>ping 10.19.8.85 Resultado: Reply from 10.19.8.85: bytes=32 time=14ms TTL=127 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:b::50	Se configura la ip estática en PC-B y la puerta de enlace Comando: C:\>ping 2001:db8:acad:b::50 Resultado: Reply from 2001:DB8:ACAD:B::50: bytes=32 time=19ms TTL=127 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1 Bucle 0	Dirección	209.165.201.1	Comando: C:\>ping 209.165.201.1 Resultado: Reply from 209.165.201.1: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:209::1	Comando: C:\>ping 2001:db8:acad:209::1 Resultado: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Comando: C:\>ping 209.165.201.1 Resultado: Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:209::1	Comando: C:\>ping 2001:db8:acad:209::1 Resultado: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.
	R1, G0/0/1.2	Dirección	10.19.8.1	Comando: C:\>ping 10.19.8.1 Resultado: Reply from 10.19.8.1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:a: :1	Comando: C:\>ping 2001:db8:acad:a::1 Resultado: Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	Comando: C:\>ping 10.19.8.65 Resultado: Reply from 10.19.8.65: bytes=32 time=1ms TTL=255 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:b: :1	Comando: C:\>ping 2001:db8:acad:b::1 Resultado: Reply from 2001:DB8:ACAD:B::1: bytes=32 time=4ms TTL=255 Resultado exitoso, si hay conexión.
	R1, G0/0/1.4	Dirección	10.19.8.97	Comando: C:\>ping 10.19.8.97 Resultado: Reply from 10.19.8.97: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.

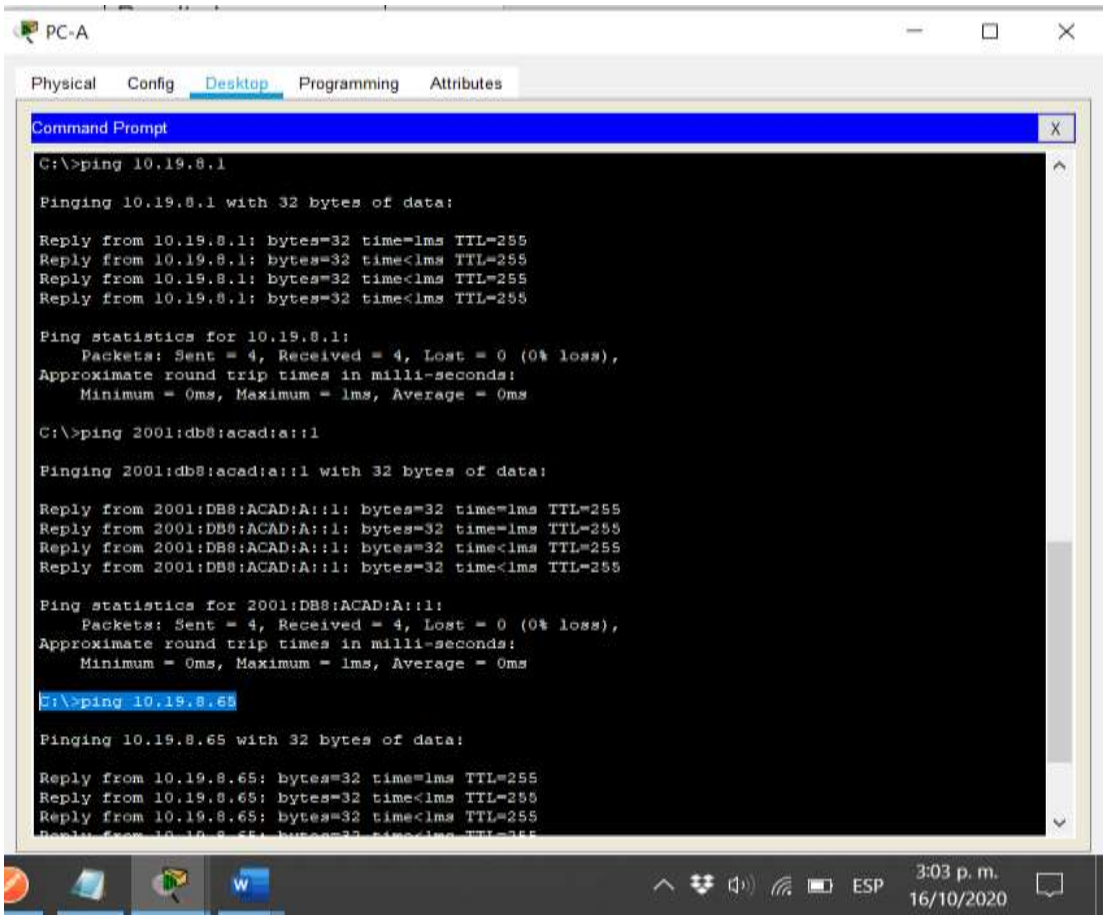
Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c: :1	Comando: C:\>ping 2001:db8:acad:c::1 Resultado: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Resultado exitoso, si hay conexión.
	S1, VLAN 4	Dirección	10.19.8.98	Comando: C:\>ping 10.19.8.98 Resultado: Reply from 10.19.8.98: bytes=32 time=11ms TTL=254 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:c: :98	Comando: C:\>ping 2001:db8:acad:c::98 Resultado: Reply from 2001:DB8:ACAD:C::98: bytes=32 time=8ms TTL=254 Resultado exitoso, si hay conexión.

Desde	A	de Internet	Dirección IP	Resultados de ping
	S2, VLAN 4	Dirección	10.19.8.99	Comando: C:\>ping 10.19.8.99 Resultado: Reply from 10.19.8.99: bytes=32 time<1ms TTL=254 Resultado exitoso, si hay conexión.
		IPv6	2001:db8:acad:c::99	Comando: C:\>ping 2001:db8:acad:c::99 Resultado: Reply from 2001:DB8:ACAD:C::99: bytes=32 time=1ms TTL=254 Resultado exitoso, si hay conexión.

1.16 EVIDENCIA GRAFICA DE VERIFICACIÓN DE CONEXIÓN EL LA RED

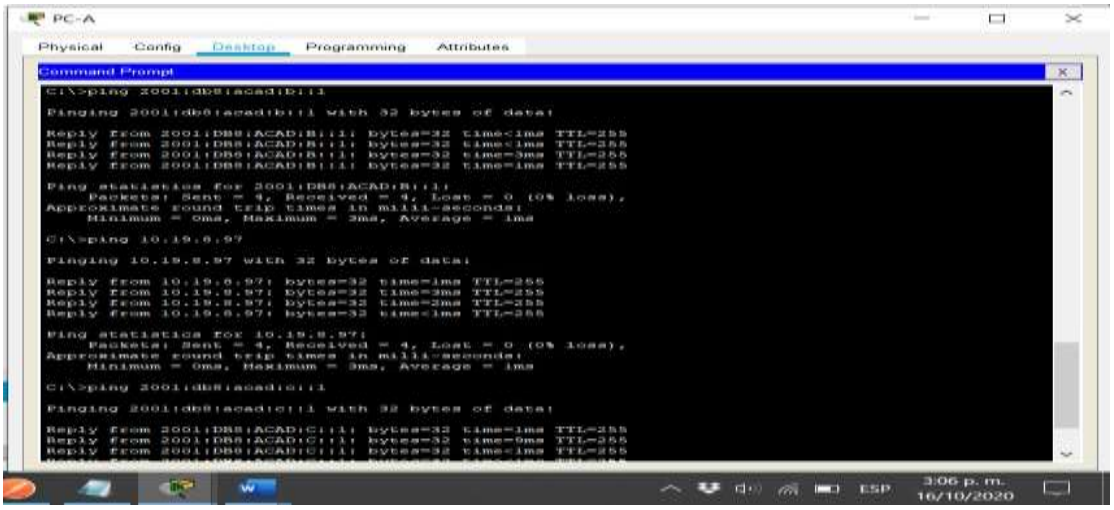
A continuación, se hace ping desde PC-A hacia las diferentes direcciones ip para probar el correcto funcionamiento de la conexión en la red:

Figura 6. Ping desde PC-A hacia 10.19.8.1, 2001:db8:acad:a::1, 10.19.8.65



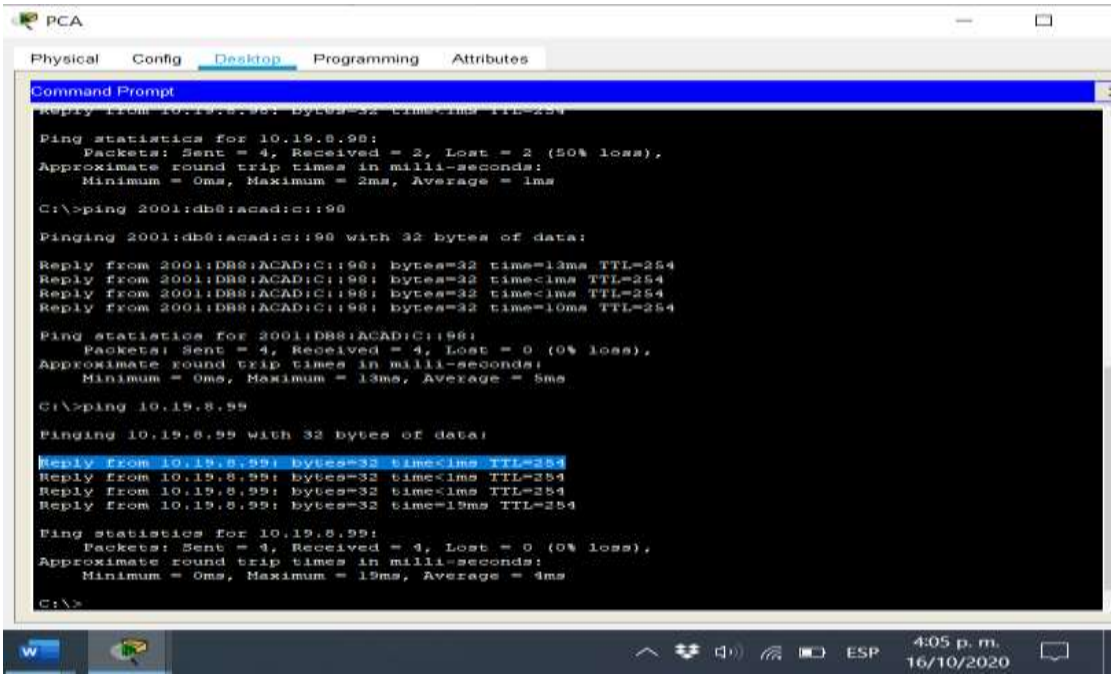
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-A hacia las direcciones 10.19.8.1, 2001:db8:acad:a::1 y 10.19.8.65 en un tiempo promedio de 1 milisegundo; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 7. Ping desde PC-A hacia 2001:db8:acad:b::1, 10.19.8.97, 2001:db8:acad:c::1



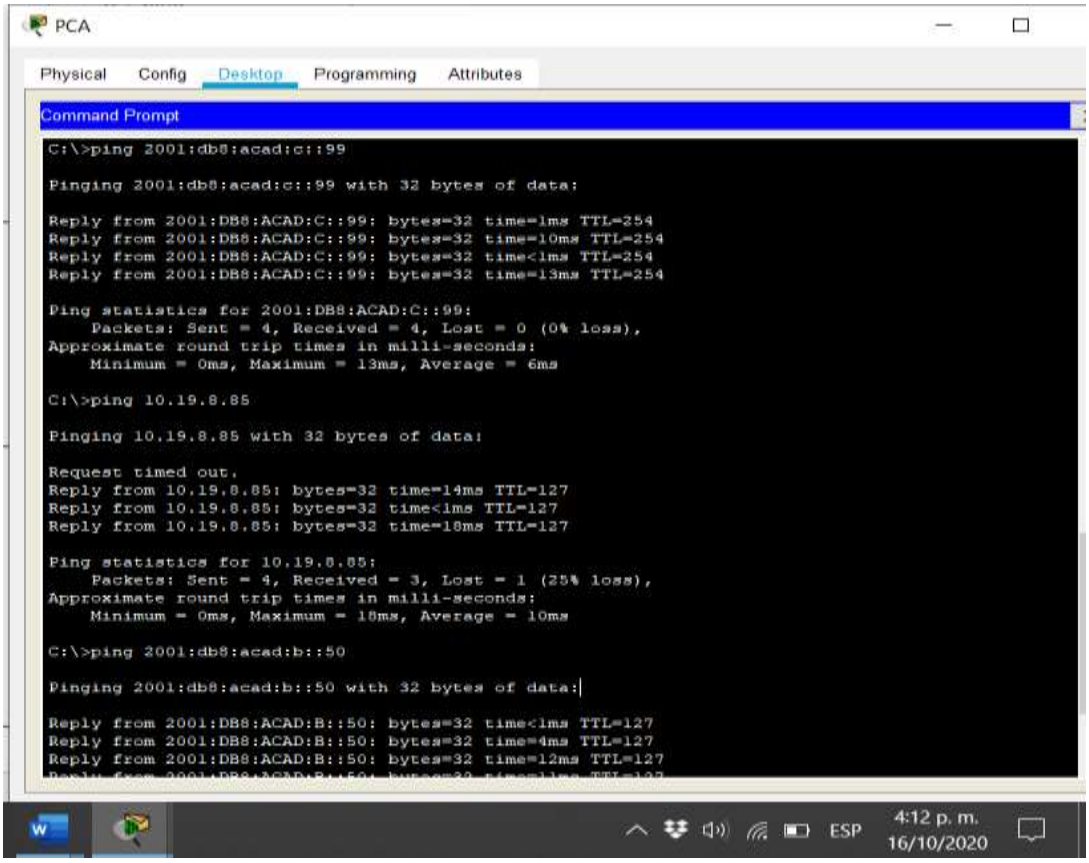
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-A hacia las direcciones 2001:db8:acad:b::1, 10.19.8.97 y 2001:db8:acad:c::1 en un tiempo promedio de 1 milisegundo; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 8. Ping desde PC-A hacia 10.19.8.98, 2001:db8:acad:c::98, 10.19.8.99



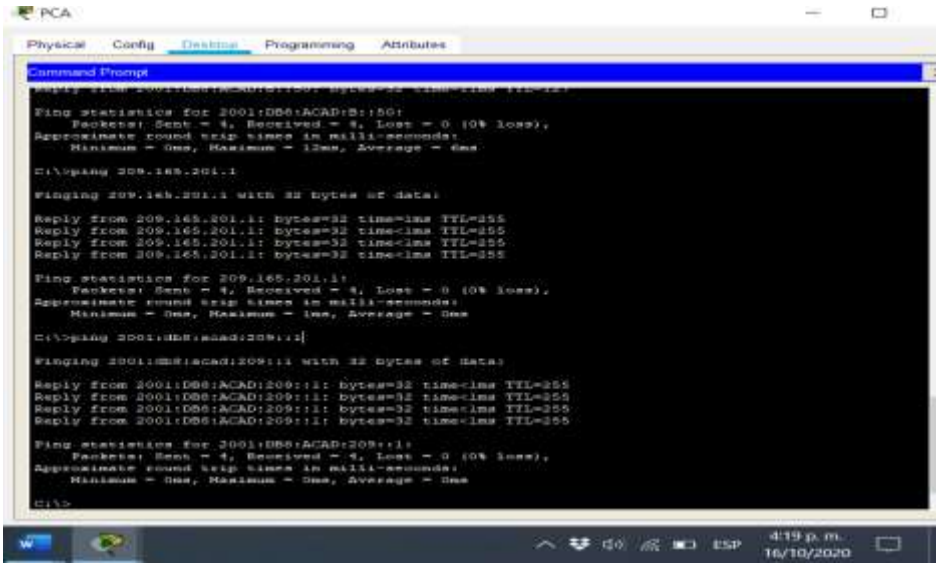
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-A hacia las direcciones 10.19.8.98, 2001:db8:acad:c::98 y 10.19.8.99 en un tiempo promedio de 4 milisegundos; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 9. Ping desde PC-A hacia 2001:db8:acad:c::99, 10.19.8.85, 2001:db8:acad:b::50



Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-A hacia las direcciones 2001:db8:acad:c::99, 10.19.8.85 y 2001:db8:acad:b::50 en un tiempo promedio de 7 milisegundos; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

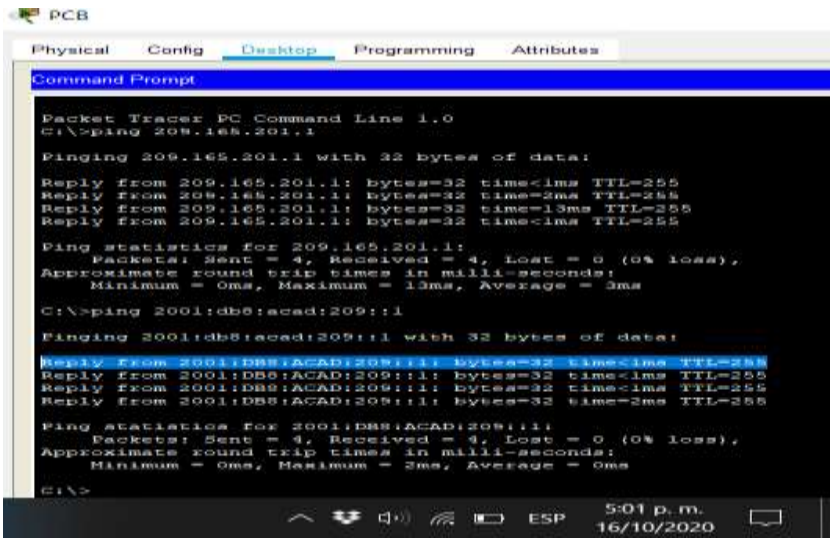
Figura 10. Ping desde PC-A hacia 209.165.201.1, 2001:db8:acad:209::1



Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-A hacia las direcciones 209.165.201.1 y 2001:db8:acad:209::1 en un tiempo promedio de 0 milisegundos; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

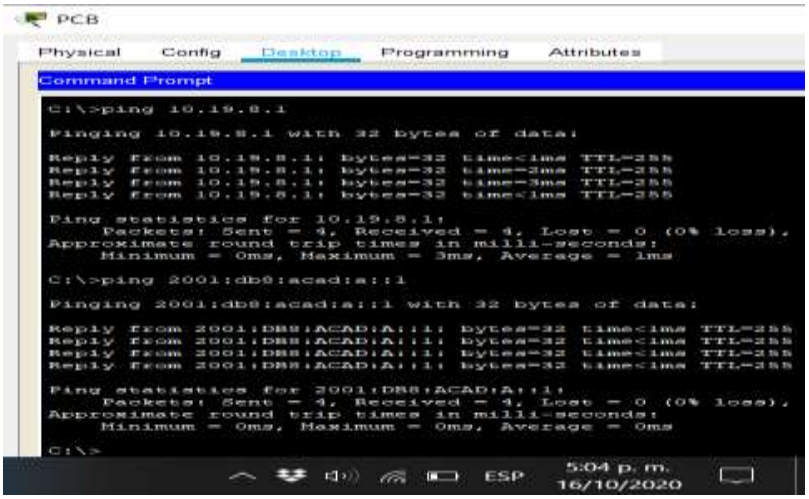
A continuación, se ejecutan las pruebas de conexión desde el PC-B hacia las diferentes direcciones Ip definidas en la tabla de verificación.

Figura 11. Ping desde PC-B hacia 209.165.201.1, 2001:db8:acad:209::1



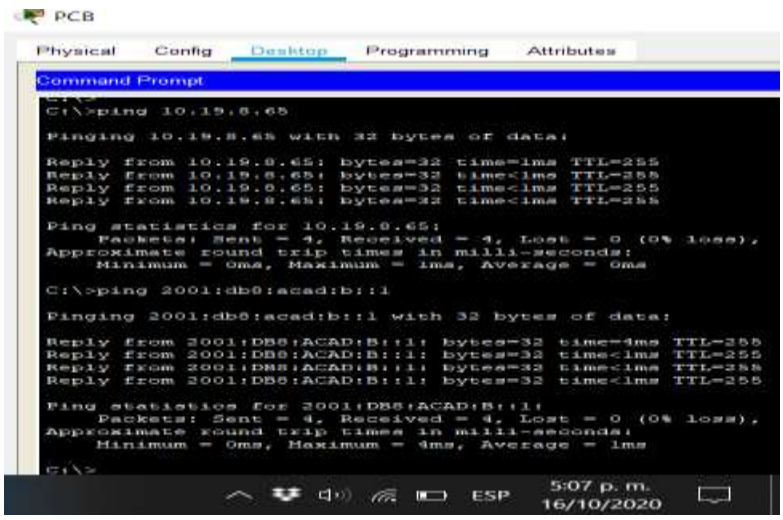
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 209.165.201.1 y 2001:db8:acad:209::1 en un tiempo promedio de 2 milisegundos; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 12. Ping desde PC-B hacia 10.19.8.1, 2001:db8:acad:a::1



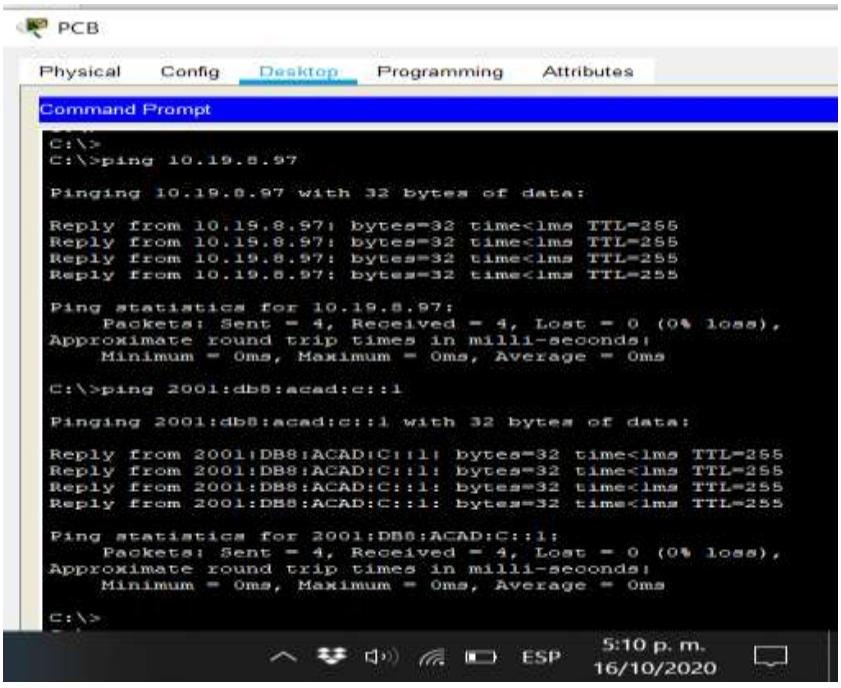
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 10.19.8.1 y 2001:db8:acad:a::1 en un tiempo promedio de 1 milisegundo; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 13. Ping desde PC-B hacia 10.19.8.65, 2001:db8:acad:b::1



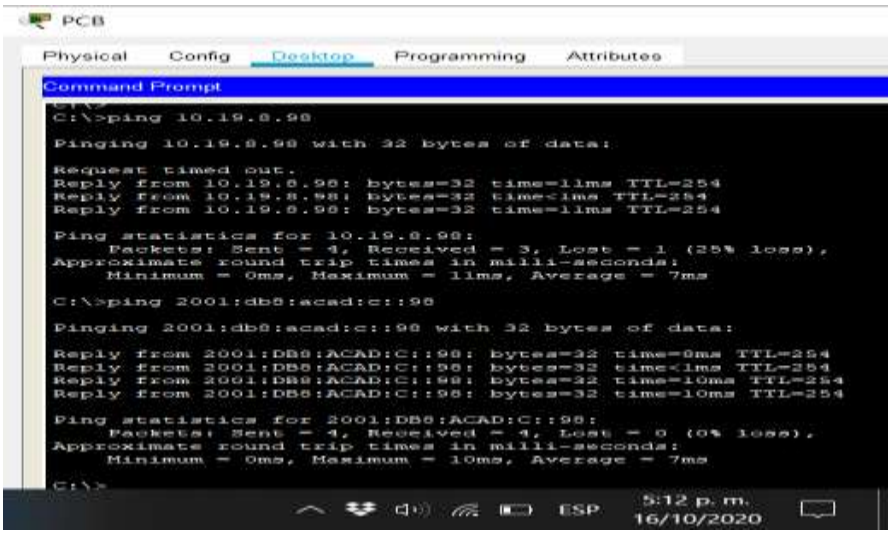
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 10.19.8.65 y 2001:db8:acad:b::1 en un tiempo promedio de 1 milisegundo; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 14. Ping desde PC-B hacia 10.19.8.97, 2001:db8:acad:c::1



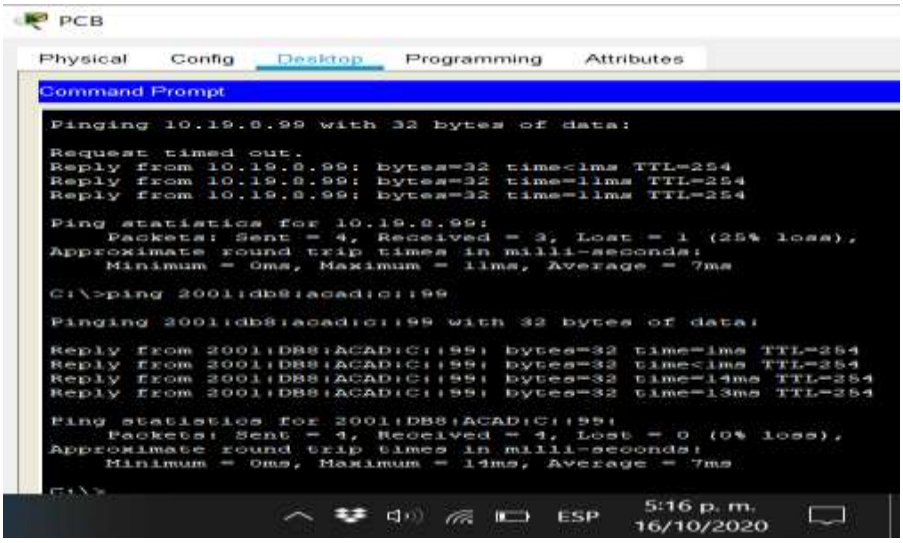
Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 10.19.8.97 y 2001:db8:acad:c::1 en un tiempo promedio de 0 milisegundos; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 15. Ping desde PC-B hacia 10.19.8.98, 2001:db8:acad:c::98



Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 10.19.8.98 y 2001:db8:acad:c::98 en un tiempo promedio de 7 milisegundos y un time out; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

Figura 16. Ping desde PC-B hacia 10.19.8.99, 2001:db8:acad:c::99



Descripción: En este caso se observa que se enviaron y luego se recibieron 4 paquetes de 32 bytes desde PC-B hacia las direcciones 10.19.8.99 y 2001:db8:acad:c::99 en un tiempo promedio de 7 milisegundos y un time out; al evidenciar la respuesta desde las direcciones Ip definidas se comprueba que si hay una conexión exitosa.

2 ESCENARIO 2

Figura 17. Escenario 2

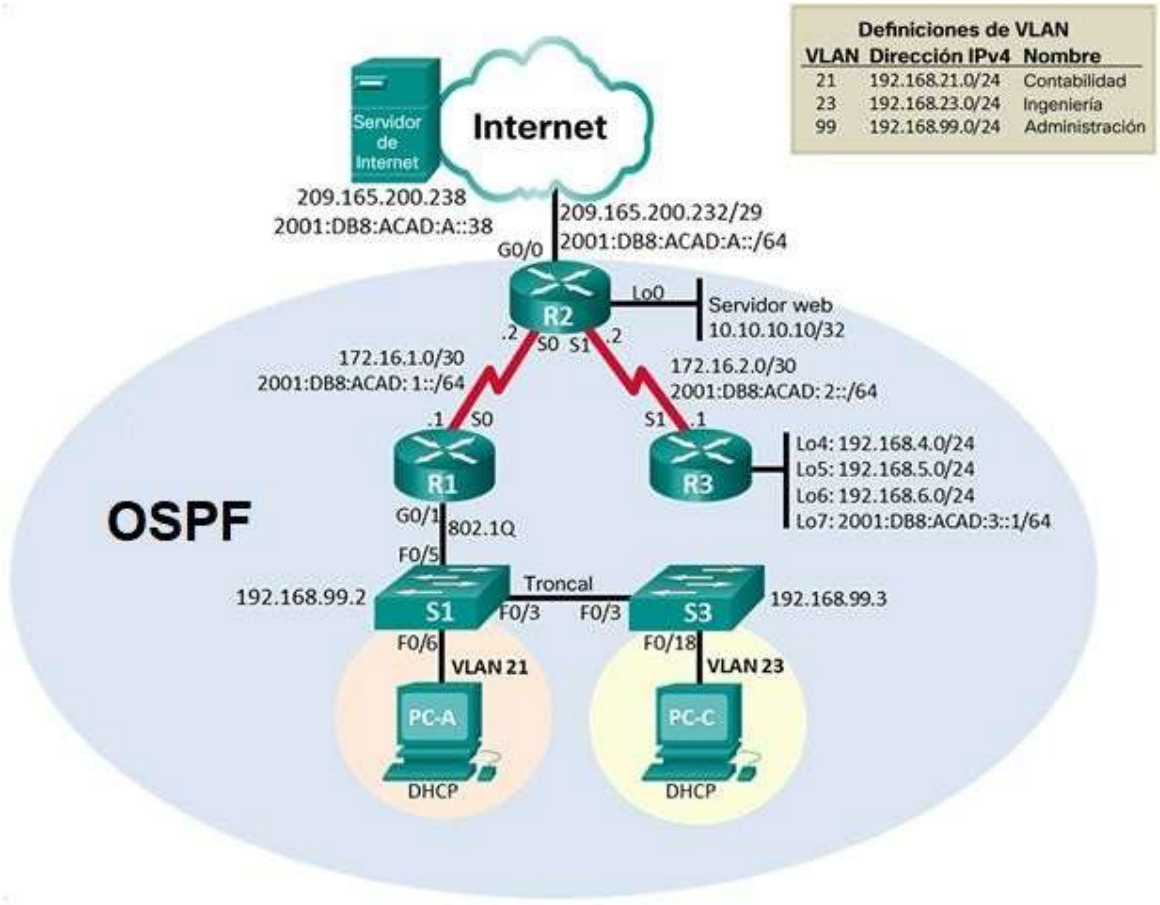
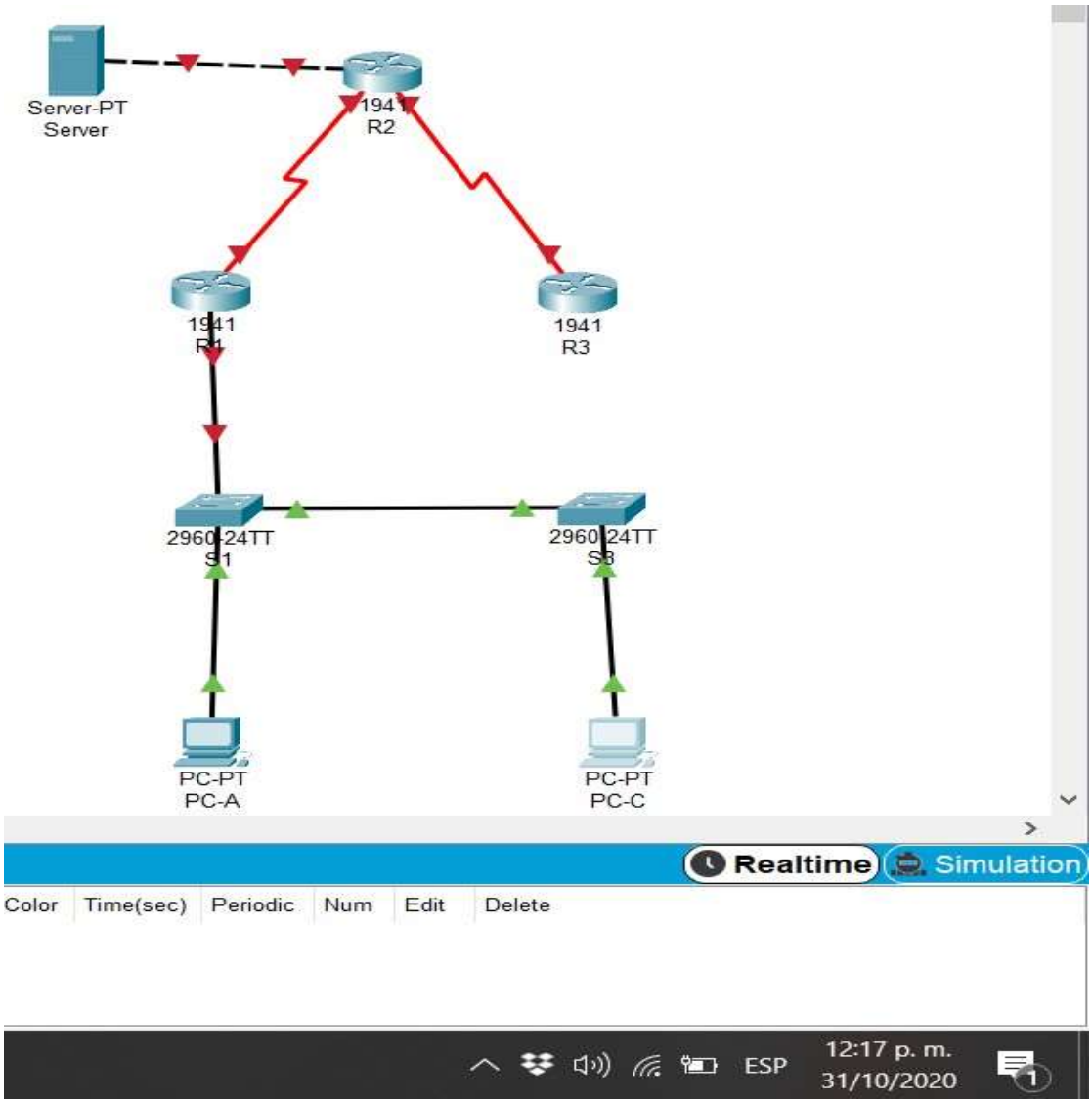


Figura 18. Simulación de escenario 2 en Packet Tracer



2.1 CREACIÓN DE LA TOPOLOGÍA

Se crea la topólogia utilizando los siguientes componentes:

-Router 1941
-Switch 2960
-PC Descktop

2.2 INICIALIZACIÓN Y RECARGA DE LOS ROUTERS Y SWITCHES

Se realiza limpieza de la configuración inicial del router y switches ya que estos dispositivos, aunque vienen con una configuración de fabrica, se deben de borrar las configuraciones para empezar desde cero a configurarlo según sea la necesidad.

Tabla 16. Recarga de router

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

Esta tabla muestra la eliminación de la configuración inicial y recarga de los router y switch de la red.

2.3 CONFIGURACIÓN DE LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

A continuación, se muestra la configuración de direccionamiento de red del servidor que se va a utilizar.

Tabla 17. Configuración del servidor

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

Esta tabla muestra la configuración de red que debe tener el servidor de la red.

A continuación, se configura la contraseña y cifrado en R1 y luego se configura el direccionamiento Ip en las interfaces correspondientes.

Tabla 18. Configuración del router R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Mensaje MOTD	R1(config)#banner motd

Interfaz S0/0/0	Establezca la descripción R1(config)#int s0/0/0 R1(config-if)#description Conexion a R2 Establecer la dirección IPv4 R1(config-if)#ip address 172.16.1.1 255.255.255.252 Establecer la dirección IPv6 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 Establecer la frecuencia de reloj en 128000 R1(config-if)#clock rate 128000 Activar la interfaz R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Esta tabla muestra la configuración inicial en el router R1 en cuanto a la seguridad ya que se crean y asignan contraseñas cifradas; además de asignar parámetros de sistema.

A continuación, se configura la contraseña y cifrado en R2 y luego se configura el direccionamiento Ip en las interfaces correspondientes.

Tabla 19. Configuración del router R2

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

Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd
Interfaz S0/0/0	Establezca la descripción R2(config)#int s0/0/0 R2(config-if)#description Conexion a R1 Establezca la dirección IPv4. Utilizar la R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 Activar la interfaz R2(config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción R2(config-if)#int s0/0/1 R2(config-if)#description Conexion a R3 Establezca la dirección IPv4. R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2(config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. R2(config-if)#int g0/0 R2(config-if)#description Conexion a Internet Establezca la dirección IPv4. R2(config-if)#ip address 209.165.200.233 255.255.255.248 Establezca la dirección IPv6 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64. Activar la interfaz R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. R2(config-if)#int loopback 0 R2(config-if)#description Simulated Web Server Establezca la dirección IPv4. R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ipv6 route ::/0 g0/0

Esta tabla muestra la configuración inicial en el router R2 en cuanto a la seguridad ya que se crean y asignan contraseñas cifradas; además de asignar parámetros de sistema como la hora entre otros.

A continuación, se configura la contraseña y cifrado en R3 y luego se configura el direccionamiento Ip en las interfaces correspondientes.

Tabla 20. Configuración del router R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#line console 0
Contraseña de acceso a la consola	R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd %Se prohibe el acceso no autorizado.!%
Interfaz S0/0/1	Establecer la descripción R3(config)#int s0/0/1 R3(config-if)#description Conexion a R2 Establezca la dirección IPv4 R3(config-if)#ip address 172.16.2.1 255.255.255.252 Establezca la dirección IPv6. R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 Activar la interfaz R3(config-if)#no shutdown
Interfaz loopback 4	Establezca la dirección IPv4. R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5	Establezca la dirección IPv4. R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4 R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección IPv6. R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#exit
Rutas predeterminadas	Ipv4 R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 Ipv6 R3(config)#ipv6 route ::/0 s0/0/1

Esta tabla muestra la configuración inicial en el router R3 en cuanto a la seguridad ya que se crean y asignan contraseñas cifradas; además de asignar parámetros de sistema como la hora entre otros.

Se configura el switch S1 para desactivar la búsqueda automática del DNS y crear contraseñas para luego cifrarlas, lo cual permite una seguridad mucho más alta junto con el uso del protocolo SSH que también ayuda a complementar los factores de seguridad de las redes.

Tabla 21. Configuración Switch S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>en Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class

Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd

Se configura el switch S1 para desactivar la búsqueda automática del DNS y crear contraseñas para luego cifrarlas, lo cual permite una seguridad mucho más alta junto con el uso del protocolo SSH que también ayuda a complementar los factores de seguridad de las redes.

Tabla 22. Configuración Swtch S3

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

Se configura el switch S3 para desactivar la búsqueda automática del DNS y crear contraseñas para luego cifrarlas, lo cual permite una seguridad mucho más alta

junto con el uso del protocolo SSH que también ayuda a complementar los factores de seguridad de las redes.

En este paso se realiza las correspondientes pruebas de conectividad o conexión entre los dispositivos mediante el comando ping, el cual envía paquetes de un punto hacia una dirección Ip y en caso de que le sean devueltos es porque hay conexión y en caso contrario es porque no hay, además en este caso también se pretende comprobar la conexión entre dispositivos en la misma Vlan.

Tabla 23. Verificación de conectividad

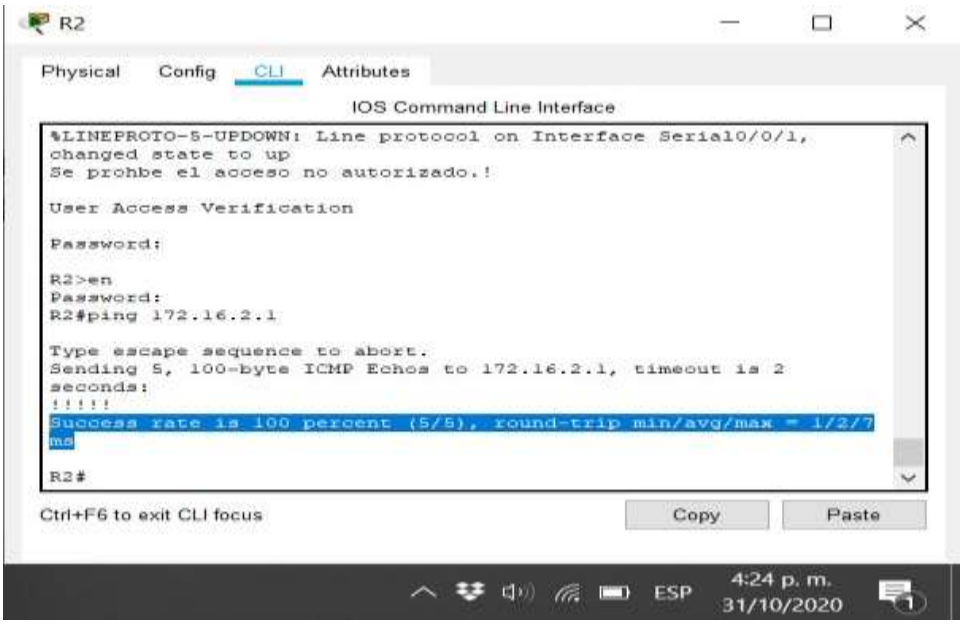
Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/19 ms
R2	R3, S0/0/1	172.16.2.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/7 ms
PC de Internet	Gateway predeterminado	209.165.200.233	Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Esta tabla define las pruebas de conectividad para este paso entre los routers y el servidor.

Figura 19. Ping desde R1 a R2

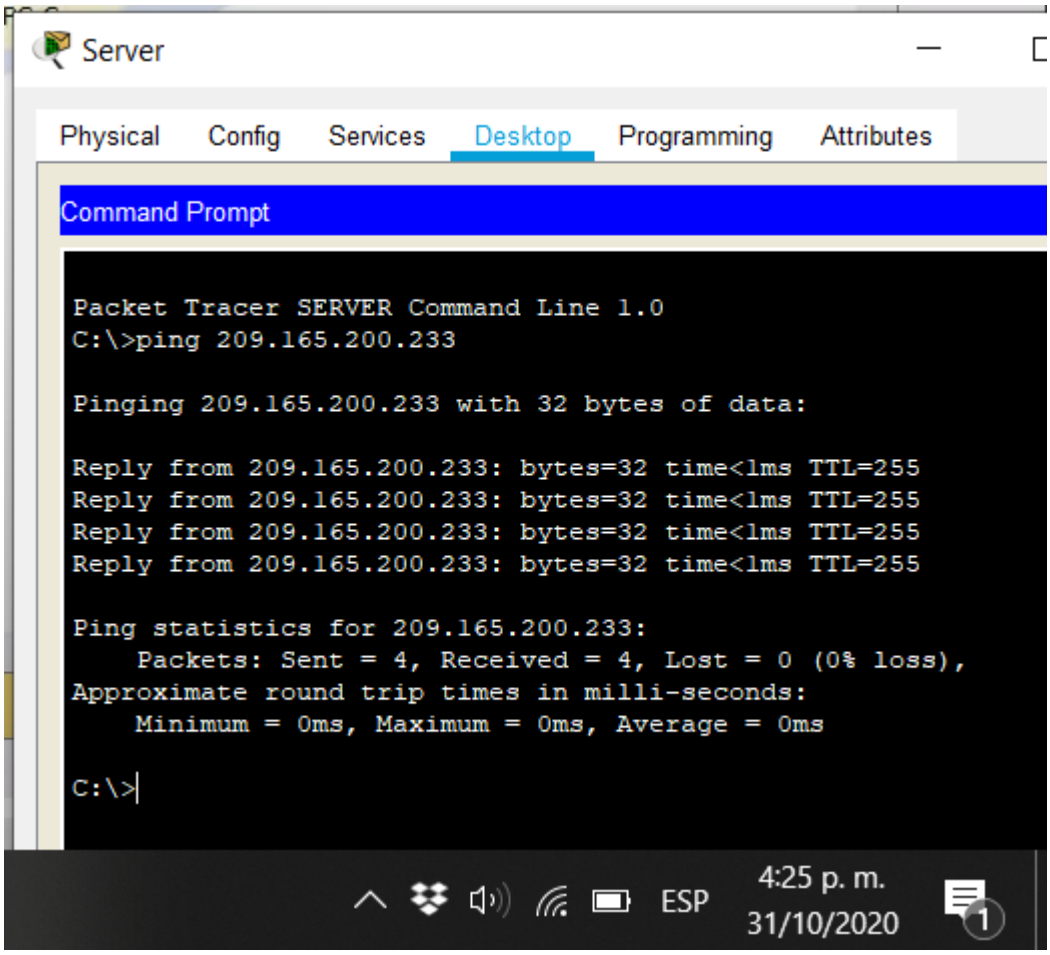
Descripción: Se hace ping desde R1 hacia R2 para verificar la conexión y en este caso se comprueba que si hay conexión.

Figura 20. Ping desde R2 a R3



Descripción: Se hace ping desde R2 hacia R3 para verificar la conexión y en este caso se comprueba que si hay conexión.

Figura 21. Ping del servidor hacia default Gateway Ip 209.165.200.233



Descripción: Se hace ping desde el servidor hacia su mismo default Gateway para verificar la conexión y en este caso se comprueba que si hay conexión.

2.4 CONFIGURACIÓN DE LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING

Tabla 24. Configuración en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#configure terminal 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)#exit
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#int 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-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Esta tabla muestra cómo se crea la base de datos de las Vlan en S1 y las interfaces predeterminadas para cada una de las Vlan.

Tabla 25. Configuración en S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#configure terminal 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)#exit
Asignar la dirección IP de administración	S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)# switchport access vlan 21
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Esta tabla muestra cómo se debe crear la base de datos de las Vlan en S3 y las interfaces predeterminadas para cada una de las Vlan.

Tabla 26. Configuración en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 Asignar la VLAN 21 R1(config-subif)#encapsulation dot1q 21 Asignar la primera dirección disponible a esta interfaz 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 R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 Asignar la VLAN 23 R1(config-subif)#encapsulation dot1q 23 Asignar la primera dirección disponible a esta interfaz 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 R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 Asignar la VLAN 99 R1(config-subif)#encapsulation dot1q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

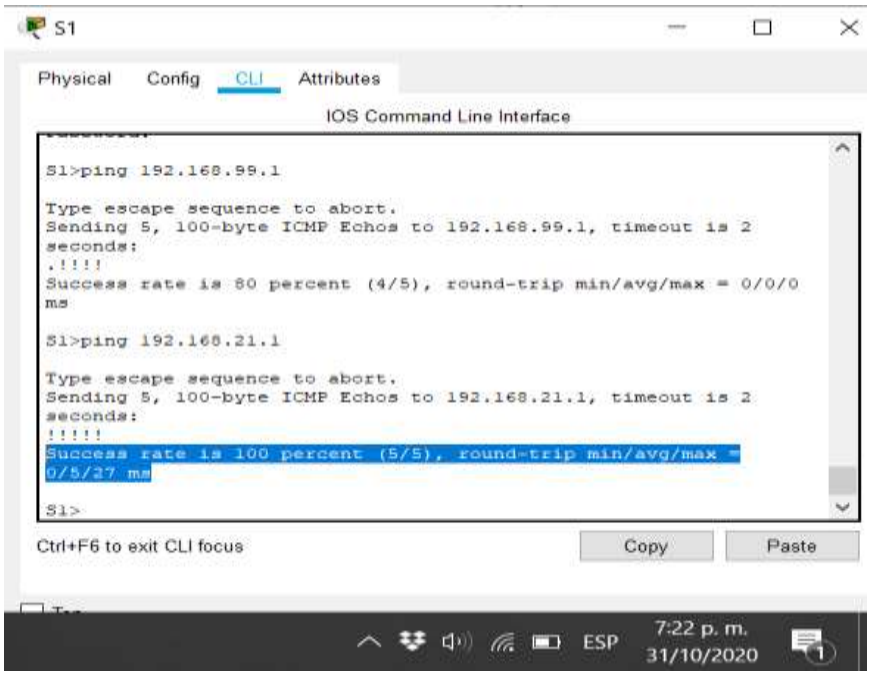
Esta tabla muestra cómo se configura las subredes correspondientes en R1 para poder identificar las Vlan creadas.

Tabla 27. Verificación de conectividad en la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms
S1	R1, dirección VLAN 21	192.168.21.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/27 ms
S3	R1, dirección VLAN 23	192.168.23.1	Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

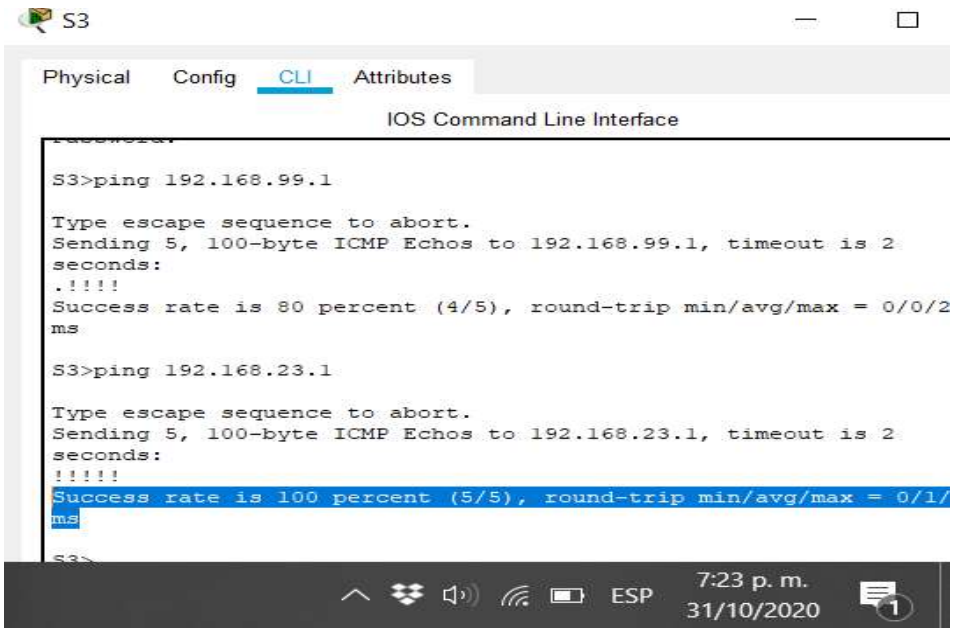
Esta tabla muestra las pruebas de conexión para verificar la configuración de las Vlan, pero en este caso no se hace desde la consola de comandos de los PC, sino desde la consola de comandos de los dispositivos switch.

Figura 22. Ping desde S1 hacia R1 Vlan 99 y Vlan 21



Descripción: Se hace ping desde S1 hacia las Vlan 99 y 21 las cuales tiene las direcciones Ip 192.168.99.1 y 192.168.21.1 respectivamente, para verificar la conexión y en este caso se comprueba que si hay conexión.

Figura 23. Ping desde S3 hacia R1 Vlan 99 y Vlan 23



Descripción: Se hace ping desde S1 hacia las Vlan 99 y 21 las cuales tiene las direcciones Ip 192.168.99.1 y 192.168.23.1 respectivamente, para verificar la conexión y en este caso se comprueba que si hay conexión.

2.5 CONFIGURACIÓN DE CONEXIÓN ENTRE DISPOSITIVOS

Tabla 28. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1#configure terminal
Anunciar las redes conectadas directamente	R1(config)#router ospf 1 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 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

Esta tabla muestra se configura la conexión en los puertos seriales de R1, ya que es la que permite conectar con los demás router, para esto se utiliza el protocolo OSPF el cual es dinámico o también se puede utilizar el protocolo RIP el cual es estático, para el caso del ejercicio se puede utilizar cualquiera de los dos ya que se conocen las direcciones Ip correspondientes.

Tabla 29. Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2#configurte terminal
Anunciar las redes conectadas directamente	R2(config)#router ospf 1 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#no auto summary
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Esta tabla muestra como se configura la conexión en los puertos seriales de R2, ya que es la que permite conectar con los demás router, para esto se utiliza el protocolo OSPF el cual es dinámico o también se puede utilizar el protocolo RIP el cual es estático, para el caso del ejercicio se puede utilizar cualquiera de los dos ya que se conocen las direcciones Ip correspondientes.

Tabla 30. Configuración OSPFv3 en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3#configure terminal
Anunciar redes IPv4 conectadas directamente	R3(config)#router ospf 1 R3(config-router)#do show ip route connected R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 172.16.4.0 0.0.3.255 area 0 R3(config-router)#network 172.16.5.0 0.0.3.255 area 0 R3(config-router)#network 172.16.6.0 0.0.3.255 area 0

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Esta tabla muestra como se configura la conexión en los puertos seriales de R3, ya que es la que permite conectar con los demás router, para esto se utiliza el protocolo OSPF el cual es dinámico o también se puede utilizar el protocolo RIP el cual es estático, para el caso del ejercicio se puede utilizar cualquiera de los dos ya que se conocen las direcciones Ip correspondientes.

Tabla 31. Verificación la información de OSPF

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R3#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R3#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R3#show ip ospf interface

Teniendo en cuenta la topología, se configuran las interfaces en R1 para la correspondiente Vlan.

Tabla 32. Configuración el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#configure terminal 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.	R1#configure terminal R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(dhcp-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)#domain-name ccna-sa.com

Esta tabla muestra la configuración teniendo en cuenta la topología, se configuran las interfaces en R2 para la correspondiente Vlan 21 y 23.

Tabla 33. Configuración la NAT estática y dinámica en el R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	R2#configure terminal R2(config)#username webuser privilege 15 secret cisco12345
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 authentication local
Crear una NAT estática al servidor web.	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 R2(config-if)#exit

Configurar la NAT dinámica dentro de una ACL privada	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: 209.165.200.225 **–** 209.165.200.228 R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248-
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

Esta tabla muestra la configuración en el router R2 en cuanto al protocolo NAT el cual permite reducir el numero de direcciones IP globales utilizadas en internet.

Se verifica la correcta configuración por medio de la configuración de los PC de la red, lo cuales deben de tomar la configuración del direccionamiento IP de forma dinámica, que para el caso fue exitoso el resultado y se evidencia en las imágenes.

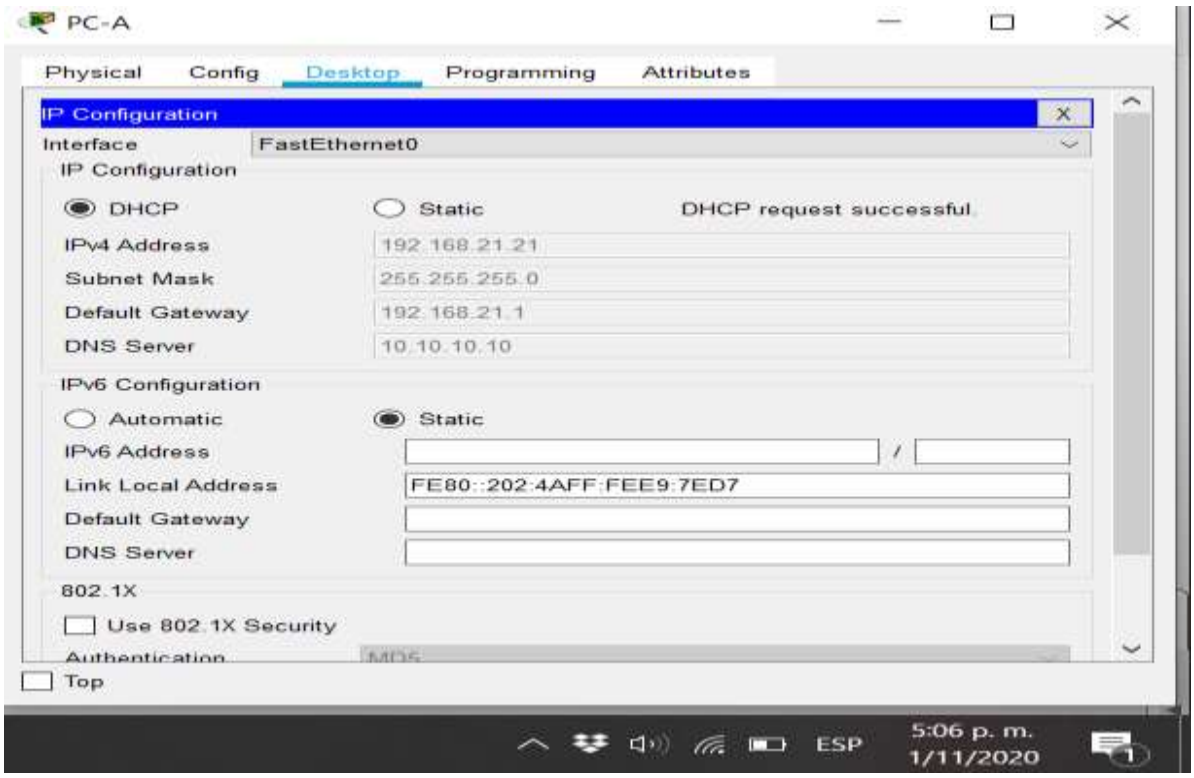
Tabla 34. Verificación el protocolo DHCP y la NAT estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso (Figura 24)
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso (Figura 25)
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso (Figura 26)

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**	Fallido (Figura 27)

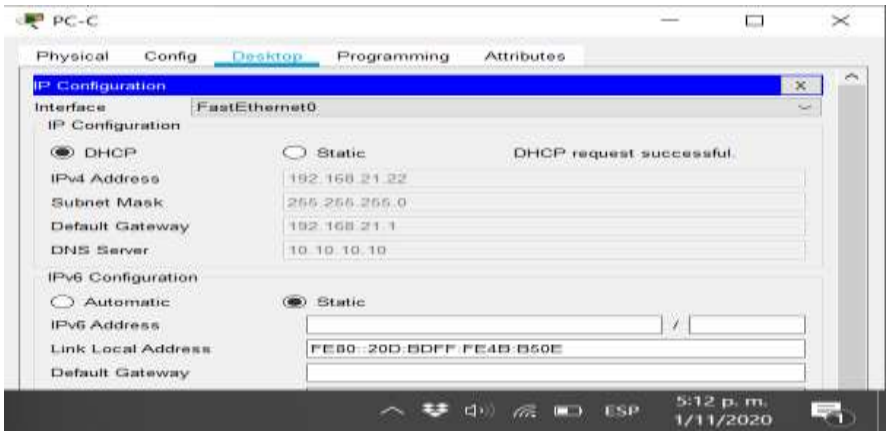
Esta tabla muestra las verificaciones de red que se deben hacer y su correspondiente resultado y relación con la imagen de evidencia.

Figura 24. Verificación dirección ip en PC-A



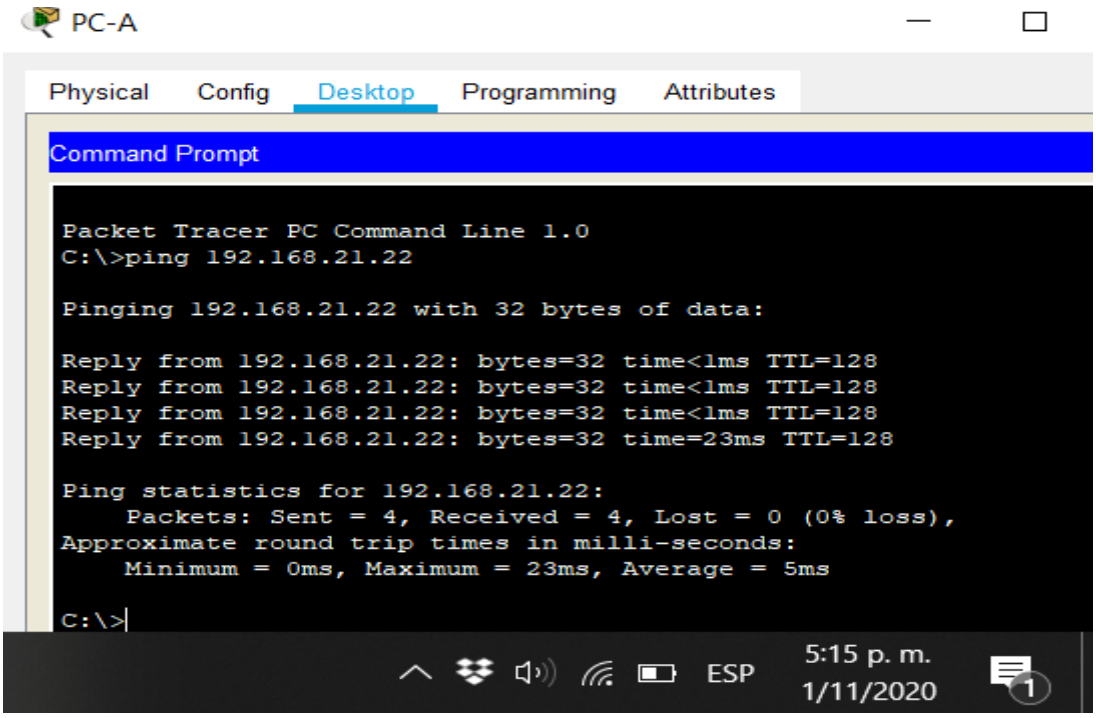
Descripción: Se verifica la configuración de direccionamiento Ip en PC-A la cual debe corresponder a la red en este caso a la Vlan 21.

Figura 25. Verificación dirección ip en PC-C



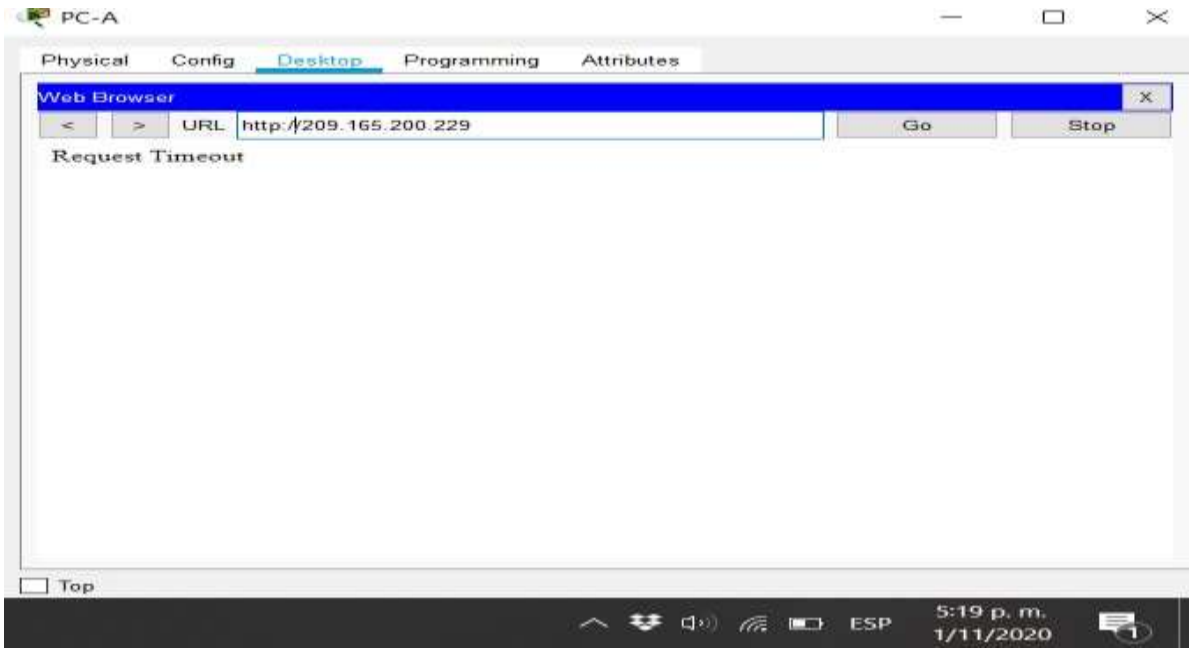
Descripción: Se verifica la configuración de direccionamiento Ip en PC-C la cual debe corresponder a la red en este caso a la Vlan 21.

Figura 26. Ping desde PC-A hacia PC-C



Descripción: Se verifica la conexión entre PC-A y PC-C los cuales se encuentran en la misma Vlan, por medio del comando ping hacia la dirección Ip 192.168.21.22 que corresponde a PC-C.

Figura 27. Acceso desde PC-A al servidor Ip 209.165.200.229



Descripción: Se verifica que el servidor este funcionando y se pueda acceder a el desde PC-A para lo cual desde PC-A se dirige hacia el escritorio luego se abre el navegador web y en la barra de navegación que se encuentra en la parte superior se digita la dirección Ip del servidor que en este caso es 209.165.200.229 acompañado del protocolo http. En este caso no funciono porque packet tracer no soporta el comando ip http server, pero en la vida real debe servir y ser funcional.

2.6 CONFIGURACIÓN DE NTP EN R1 Y R2

Se configura el protocolo NTP en la red para que todos los dispositivos cuenten con la misma hora y fecha.

Tabla 35. Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 17:23:00 01 november 2020
Configure R2 como un maestro NTP.	R2(config)#ntp master 5

Configurar R1 como un cliente NTP.	Servidor: **R2** R1#configure terminal 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#show ntp associations

Esta tabla muestra la configuración del protocolo NTP que permite configurar el sistema del dispositivo, en este caso en el router R1.

Figura 28. Asociaciones de NTP en R1

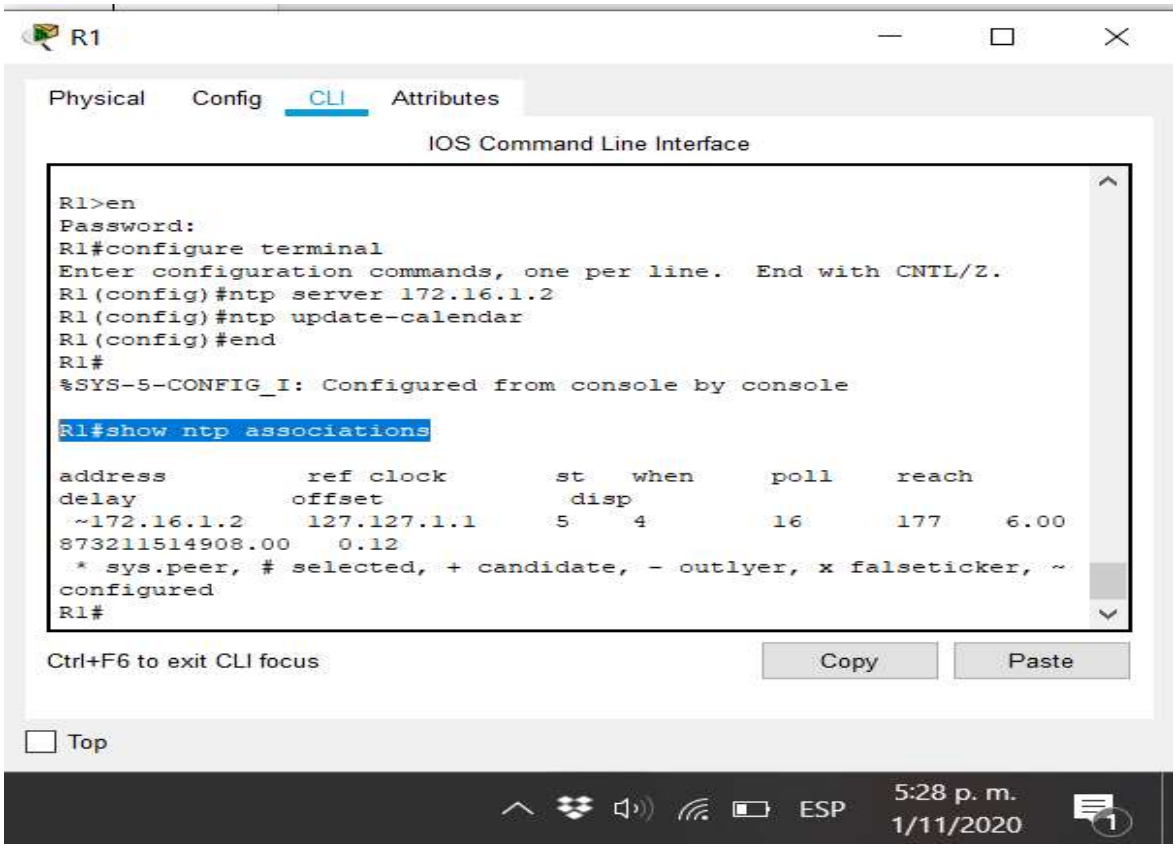
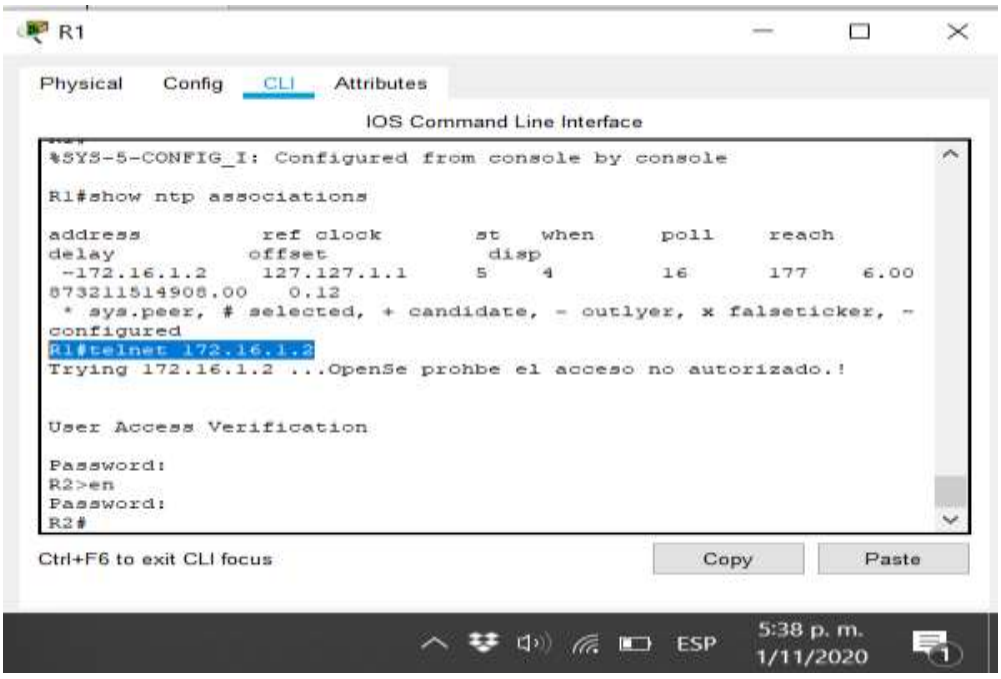


Tabla 36. Restricción del acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

Esta tabla muestra la configuración en las líneas VTY en el router R1 las cuales se utilizan para conexiones de telnet que se van a utilizar.

Figura 29. Verificación acceso telnet desde R1 hacia R2



Descripción: Se verifica el canal de telnet desde R1 hacia R2 el cual se ejecuta con el comando telnet seguido de la dirección Ip del otro dispositivo para el caso fue de la siguiente manera: telnet 172.16.1.2.

2.7 INTRODUCCIÓN DE COMANDOS CLI PARA MOSTRAR INFORMACIÓN

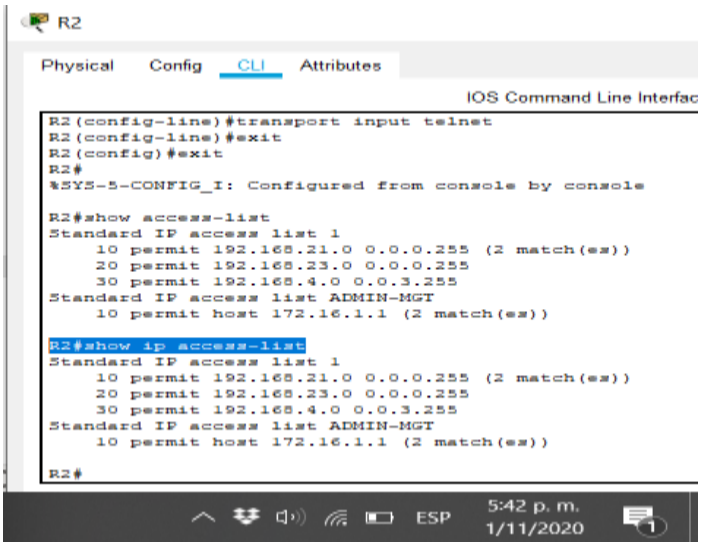
Se utilizan diferentes comandos para visualizar la configuración que se ha realizado en el dispositivo R2.

Tabla 37. Comandos CLI

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list R2#show ip access-list
Restablecer los contadores de una lista de acceso	R2#clear ip 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 ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

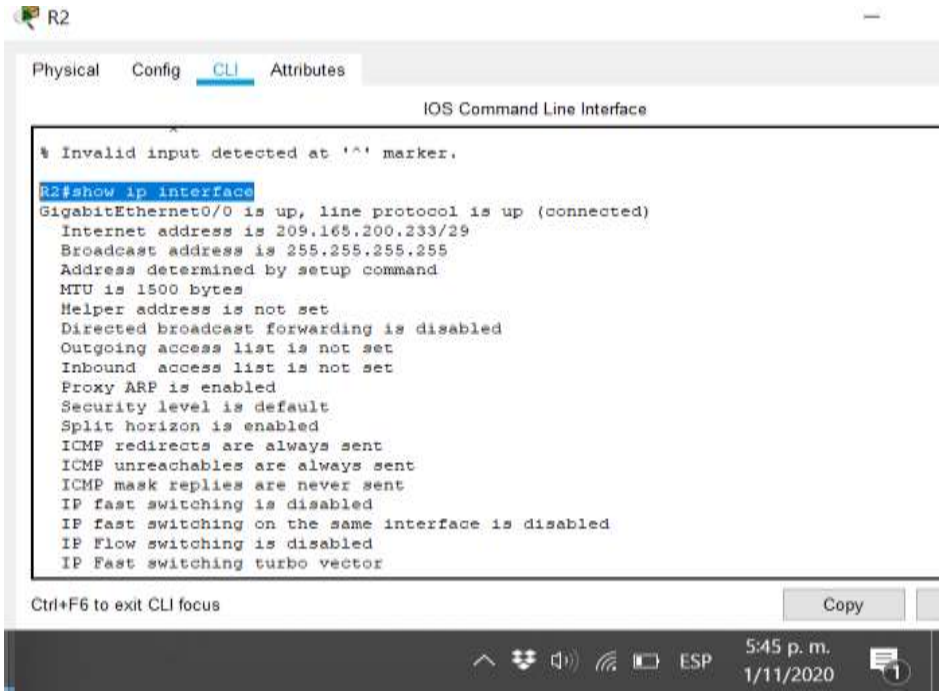
Esta tabla muestra una tarea y en frente un comando el cual se debe ejecutar para realizar dicha tarea.

Figura 30. Coincidencias recibidas en R2



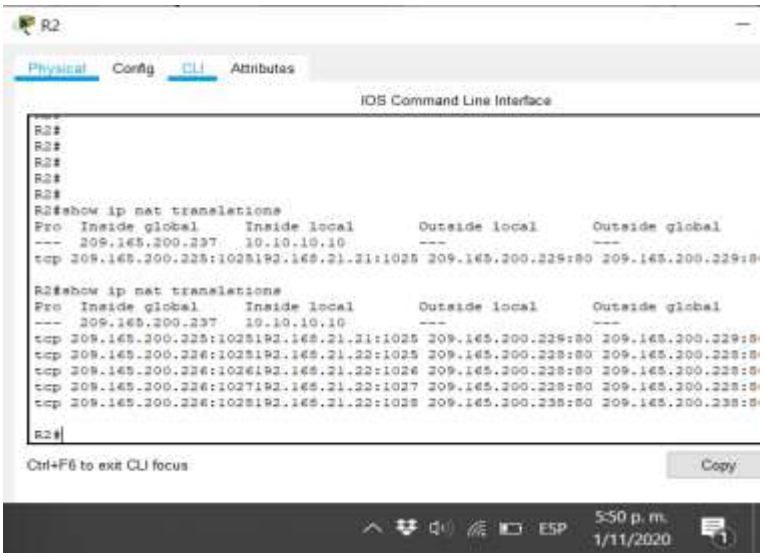
Descripción: Se muestra las interfaces que están asignadas a cada Vlan y si correspondiente dirección Ip de red Vlan.

Figura 31. Interfaces en R2



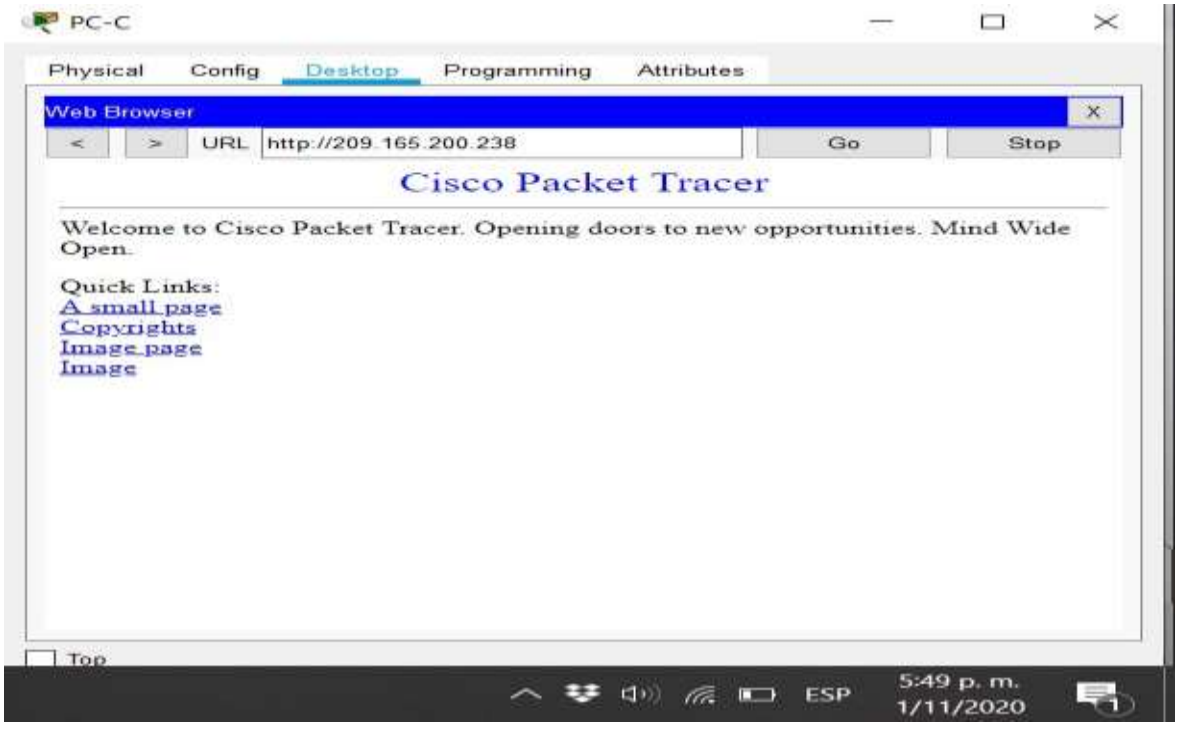
Descripción: Se muestra las interfaces asignadas que están en funcionamiento y su correspondiente dirección Ip.

Figura 32. Traducciones NAT en R2



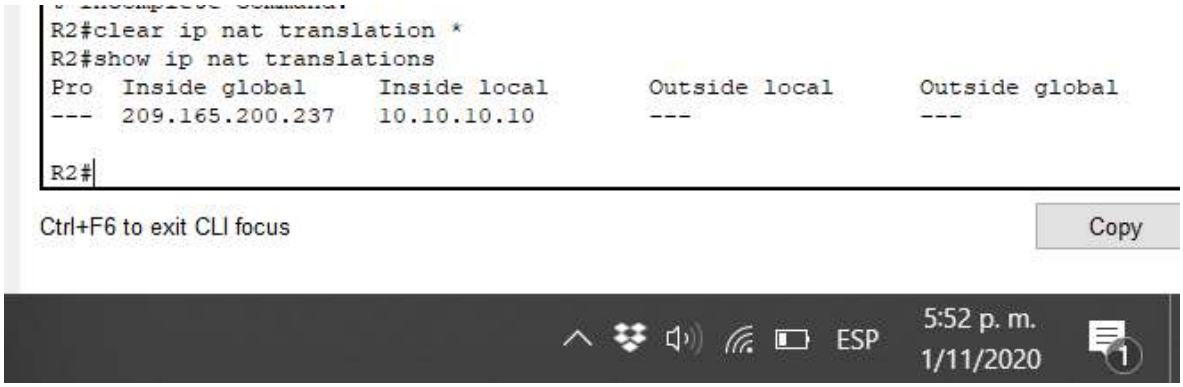
Descripción: Se verifica con que dirección Ip se está saliendo a internet desde R2 ya que es el router que conecta a internet al resto de dispositivos en la red excepto el servidor, como se sabe el protocolo NAT permite reducir el número de direcciones Ip a nivel global, esto hace que sea muy utilizado.

Figura 33. Acceso desde PC-C a servidor web



Descripción: Se verifica el acceso al servidor desde PC-C, para lo cual hay que dirigirse al escritorio, luego al navegador y digitar la dirección Ip del servidor acompañado del protocolo http; para este caso se digito http://209.165.200.238 y se evidencia que si hay acceso desde el PC-C.

Figura 34. Limpieza de traducciones NAT en R2



3 CONCLUSIONES

Existen una gran cantidad de aspectos a tener en cuenta al momento de crear una red tanto LAN como WAN ya que si no se planea y ejecuta óptimamente puede generar un aumento en el riesgo de vulnerabilidad de la red, de los datos y de los dispositivos con sus archivos, por lo que es recomendable desde el comienzo que se empieza a configurar cualquier dispositivo, borrar la configuración de fábrica y recargarlo antes de empezar a configuración donde los primer es colocar contraseñas en mas de un nivel de acceso y siempre con cifrado lo cual hace mas difícil para quien intente adquirir los accesos; también se debe de configurar y utilizar los protocolos de seguridad ya existentes para cifrar los archivos o mensajes entre los dispositivos como el protocolo SSH; también se puede crear diferentes Vlan para proteger el accesos en una red LAN lo cual también puede hacer mas optima y segura una red.

Es muy importante y relevante el conocimiento desde el primer momento que se planea la topología de la red, ya que desde el principio debe quedar bien definida para después no tener inconvenientes ya que hay varios aspectos a tener en cuenta desde el tipo de dispositivos hasta el direccionamiento ip en los dispositivos, teniendo en cuenta que en muchos caso se puede utilizar redes VLAN que permiten mantener la seguridad de la información compartida únicamente entre los dispositivos que son asignados de la VLAN; esta es solo una de las formas de mantener la seguridad de los datos transmitidos en la red así también se encuentra el cifrado de los datos mediante el protocolo SSH para que no puedan ser espiados al momento en que se envían. Además, el buen diseño de la topología permite instalar una red con el mejor rendimiento que a largo plazo es más fácil de hacer mantenimiento.

4 BIBLIOGRAFIA

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

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

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

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

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

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11.

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

5 ANEXOS

Simulador del escenario #1:
https://drive.google.com/file/d/1jf39vN3xG_Va0mOiEW0_uP-g98gUboUh/view?usp=sharing

Simulador del escenario #2:
https://drive.google.com/file/d/1O9O_As-MC2Wi3SoKcUyF9fVLllSCyXyj/view?usp=sharing

Articulo:
https://drive.google.com/file/d/16SScMdCWgDDnMW7NWEXMH8Z9FdNuoEqk/view?usp=sharing