Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnología CISCO

Dahianna Vanesa Ospina

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnologías e Ingenierías
Ingeniería de Sistemas
Medellín, Antioquia
2020

Solución de dos escenarios presentes en entornos corporativos bajo el uso de tecnología CISCO

Dahianna Vanesa Ospina

Trabajo de la opción de grado para optar al título de Ingeniero de Sistemas

Asesor
Juan Carlos Vesga Ferreira
Docente

Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnologías e Ingenierías
Ingeniería de Sistemas
Medellín, Antioquia
2020

Tabla de contenidos

Lista de tablas

Lista de graficas

Resumen

Teniendo en cuenta el papel que desempeña en la actualidad la tecnología en el desarrollo global de la economía a nivel mundial, hace que cada vez más las Organizaciones inviertan en una arquitectura tecnológica segura y robusta, que le permitan garantizar la seguridad, confiabilidad y disponibilidad de la información.

Es por ello que los escenarios de redes requieren un diseño basado en la implementación de protocolos de seguridad que garanticen una conectividad optima entre sus dispositivos, permitan restricción de comunicación no requerida, métricas de enrutamiento, análisis de tráfico y autenticación de seguridad que brinden confidencialidad de los datos que circulan a través de la red.

Haciendo uso de la herramienta de simulación PACKET TRACER, de CISCO Networking Academy, se lleva a cabo la práctica de los conocimientos adquiridos, mediante el desarrollo de dos escenarios, que plantean la configuración de redes pequeñas, que deben permitir conectividad IPv4 e IPv6, implementando configuraciones básicas de seguridad, enrutamiento entre VLAN, DHCP, Etherchannel y port-security, 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.

Abstract

Taking into account the role that technology currently plays in the global development of the world economy, it makes more and more Organizations invest in a secure and robust technological architecture, which will compromise the security, reliability and availability of the information.

That is why network scenarios require a design based on the implementation of security protocols that guarantee optimal connectivity between your devices, restriction of communication not required, routing metrics, traffic analysis and security authentication that provide confidentiality of the data circulating through the network.

Using the simulation tool PACKET TRACER, from CISCO Networking Academy, the acquired knowledge is practiced through the development of two scenarios, which propose the configuration of small networks, which must allow IPv4 and IPv6 connectivity, implementing basic security configurations, routing between VLANs, DHCP, Etherchannel and port-security, OSPF dynamic routing protocol, Dynamic Host Configuration Protocol (DHCP), static and dynamic network address translation (NAT), checklists Server / Client Access Protocol (ACL) and Network Time Protocol (NTP).

Glosario

VLAN: (virtual local area network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

WLAN: siglas inglesas de Wireless Local Área Network, que es español significa Red de Área Local Inalámbrica.

OSPF: Protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

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

PAT (Port Address Translation): Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.

DNS: (Domain name system, sistema de nombre de dominio) servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio.

PING: Comando utilizado para verificar conectividad en una interfaz de red.

LAN (Local Area Network) es una red que conecta uno o más ordenadores dentro de un ámbito pequeño y limitado.

MÉTRICA: Es un valor que se asigna a una ruta IP para una interfaz de red determinada que identifica el costo asociado con el uso de esa ruta.

PROTOCOLO DE ENRUTAMIENTO: Conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento.

Introducción

Mediante el desarrollo del presente trabajo que busca afianzar los conocimientos adquiridos en el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), a través de la configuración de dos escenarios: El primero corresponde a una pequeña red, debe admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados, el router y los switches deben administrarse de forma segura, realizándose configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security. En el segundo escenario se implementa 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.

Teniendo en cuenta que uno de los factores más primordiales en el diseño de una red es garantizar seguridad y disponibilidad, se hace necesario la configuración adecuada de los dispositivos de red, a través de la implementación de protocolos seguros que permitan la comunicación necesaria y denieguen la no requerida, filtrando el tráfico de red para optimizar los recursos, permitiendo análisis de comportamiento y métricas de enrutamiento, diseñando políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, que permite dar soluciones de red y conectividad escalables, a través del uso de enrutamiento y conmutación de paquetes en redes LAN y WAN.

Objetivos

OBJETIVO GENERAL:

Realizar la configuración de las redes acorde a los escenarios propuestos, utilizando la herramienta Packet Tracer de simulación LAN/WAN.

OBJETIVOS ESPECÍFICOS:

Establecer de manera correcta los dispositivos de networking que forman parte de la Topologías de los escenarios y realizar el diseño de red acorde a los requerimientos planteados.

Realizar la configuración de los dispositivos según los lineamientos expuestos para lograr la conectividad de extremo a extremo.

Realizar el análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

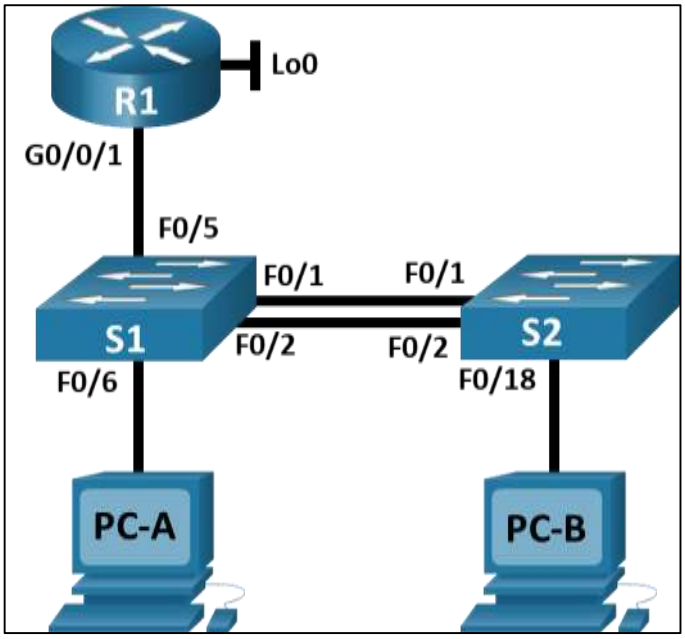
Identificar las herramientas de supervisión y protocolos de administración de red disponibles en el IOS.

Configurar los protocolos de enrutamiento y las políticas de seguridad definidas conforme a cada escenario.

1 Desarrollo del escenario 1

Topología

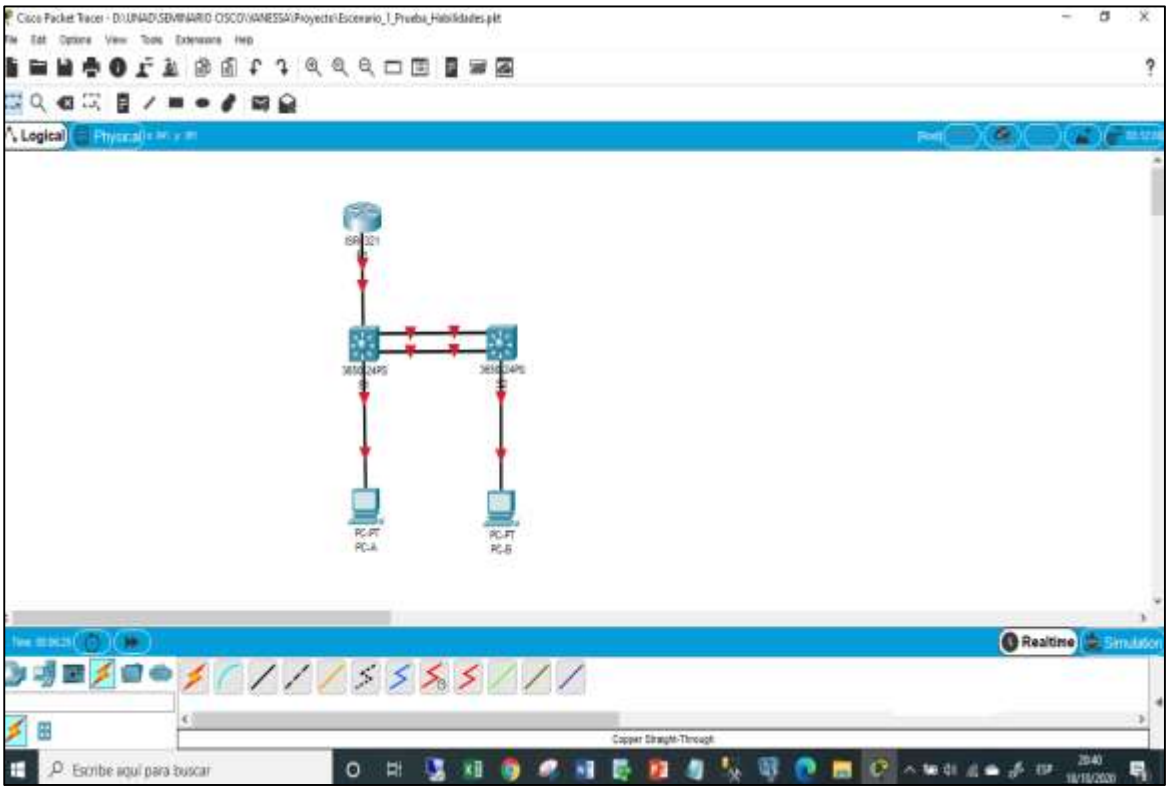
Figura 1. Topología de Red Escenario 1



Prueba de habilidades CCNA II-2020

Con base en la topología de red propuesta, se procede a realizar la configuración física del primer escenario, el cual corresponde a una pequeña red, en la que se realiza la configuración de los dispositivos: Un router, dos switch y dos equipos PC los cuales deben admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados. Igualmente, el router y los switches deben administrarse de forma segura, permitir la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 2. Topología de Red Escenario 1



Fuente Propia

1.1 Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

1.1.1 Inicializar y volver a cargar el router y los switches

Según los requerimientos del Escenario 1, se procede a realizar la configuración inicial de cada uno de los dispositivos como primer paso, borrar las configuraciones de inicio del router y de los switches, así como las VLAN y se vuelven a cargar los dispositivos, verificando con el mensaje arrojado por los dispositivos que no tienen configuración de inicio, posteriormente se realiza la configuración de la plantilla SDM verificando que admita IPv6 según sea necesario y se vuelven a cargar los switches. Estas tareas se llevan a cabo mediante el uso de los comandos descritos en la siguiente tabla.

Tabla 1. Borrado de Configuración inicial

Tarea	Comando
Borrar las configuraciones de inicio en el Router	Router>enable Router#erase startup-config

Volver a cargar el router	Router#reload
Borrar las configuraciones de inicio en los Switches	Switch>enable Switch#erase startup-config
Borrado de la Base de Datos de la VLAN en los switches	Switch#delete vlan.dat
Volver a cargar los switches	Switch#reload
Configuración de la plantilla SDM para que admita IPv6 en los switches	Switch>enable Switch#show sdm prefer

1.1.2 Configuración de R1

Posterior a la inicialización de los dispositivos, se procede a realizar la configuración básica de seguridad del Router, que incluye las tareas descritas en la en la siguiente tabla:

Tabla 2. Configuración de R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin 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

	R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd # UnAuthorized Access is prohibite!#
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)# 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)#description Management 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
Configure el Loopback0 interface	R1(config-if)#int loopback 0 R1(config-if)#ip addres 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 R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa modulus 1024 (comando invalido en packet tracer) R1(config)#crypto key generate rsa

1.1.3 Configuración de S1 y S2

Se realiza las configuraciones básicas de seguridad en los switches, se asignan los nombres según la topología (S1 y S2), se desactiva la búsqueda DNS, se asignan las contraseñas de acceso privilegiado, de consola y telnet: ciscoenpass, se crea el mensaje de acceso no autorizado, tareas que se detallan en la siguiente tabla:

Tabla 3. Configuración de S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#config term Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
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 ciscoenpass

	S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	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 S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd # UnAuthorized Access is prohibite!#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa modulus 1024(comando invalido en packet tracer) S1(config)#crypto key generate rsa
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 S1(config)#ipv6 route ::/0 2001:db8:acad:c::1

Tabla 4. Configuración de S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config term 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 ciscoenpass 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
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 # UnAuthorized Access is prohibite!#
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa modulus 1024(comando invalido en packet tracer) S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#int vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248

	S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#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 S2(config)#ipv6 route ::/0 2001:db8:acad:c::1

1.2 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Se procede a crear las VLAN, Trunking, EtherChannel, según la tabla de equivalencias propuesta para la topología de red.

1.2.1 Configuración de VLAN en S1

Tabla 5. Configuración de VLAN en S1

Tarea	**Especificación**
Crear VLAN	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)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	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 S1(config-if)#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)#interface 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	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
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 S1(config)#int range g1/0/1-2 S1(config-if-range)#no shutdown

1.2.2 Configuración de VLAN en S2

Tabla 6. Configuración de VLAN en S2

Tarea	Especificación
Crear VLAN	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)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	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
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 S2(config-if-range)#int range g1/0/1-2 S2(config-if-range)#no shutdown

1.3 Configuración soporte de host

Acorde a las indicaciones del escenario se procede a realizar el enrutamiento por defecto y a la creación de rutas predeterminadas para IPv4 e IPv6 para direccionar tráfico a la interfaz Loopback 0, creación de un grupo DHCP para VLAN 2 y VLAN 3 compuesto por las últimas 10 direcciones de la subred y creación del nombre de dominio.

1.3.1 Configuración de Enrutamiento R1

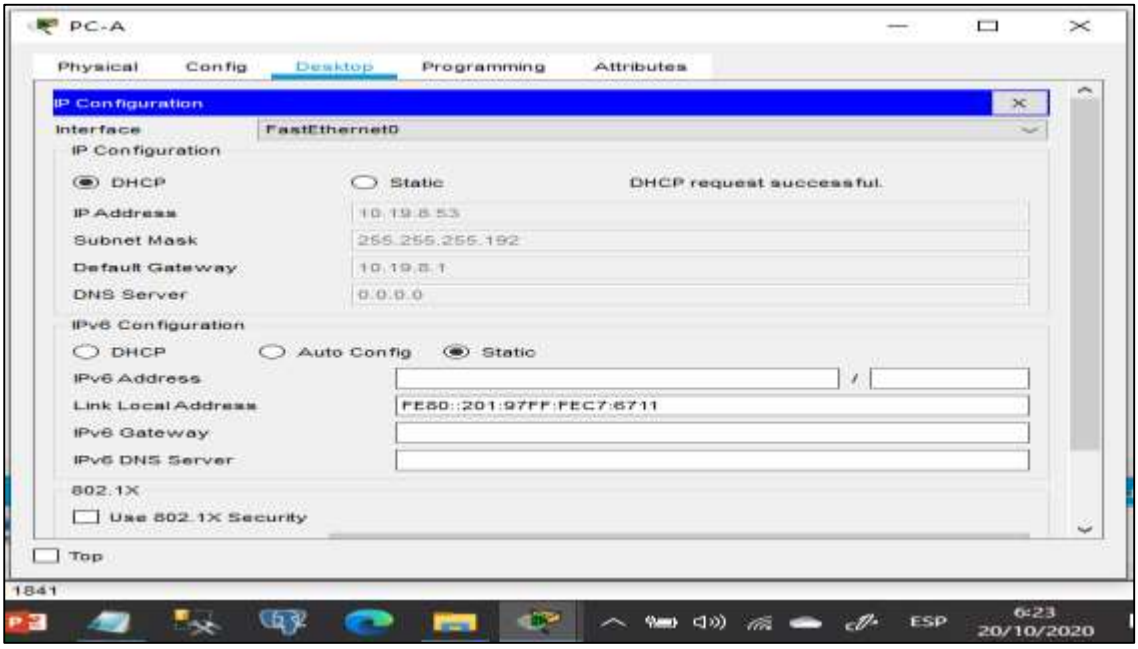
Tabla 7. Configuración de Enrutamiento R1

Tarea	**Especificación**
Configure Default Routing	R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp 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)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 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 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

1.3.2 Configuración de los PC

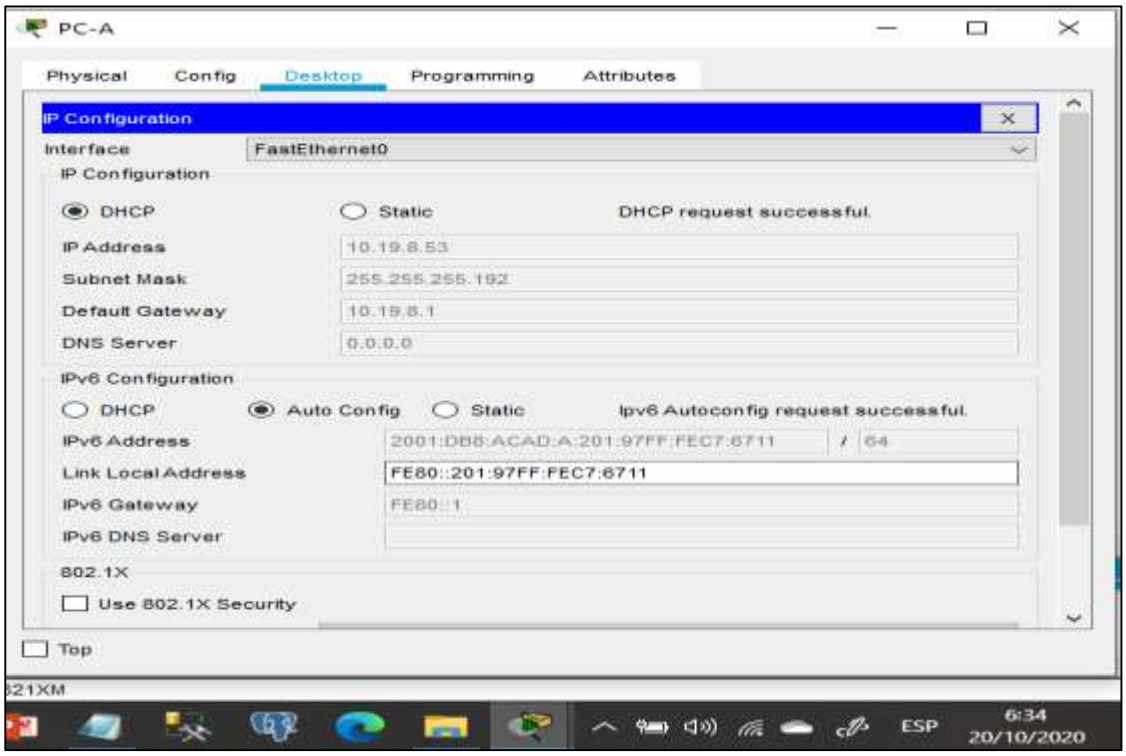
Se realiza la configuración de los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de realizar la configuración en cada PC, se procede a verificar las configuraciones de red del cada host usando el comando ipconfig /all.

Figura 3. Verificación de Configuración DHCP host PC-A



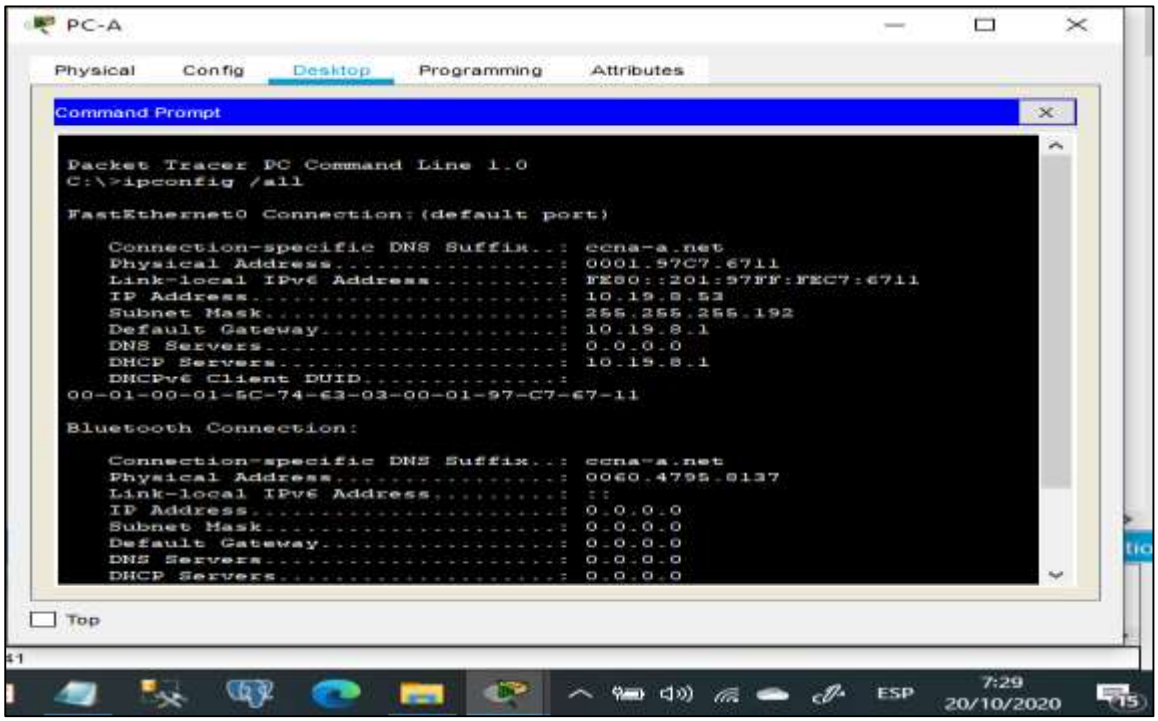
Fuente Propia

Figura 4. Asignación Estática de IPV6 y link Local PC-A



Fuente Propia

Figura 5. Configuración de red host PC-A

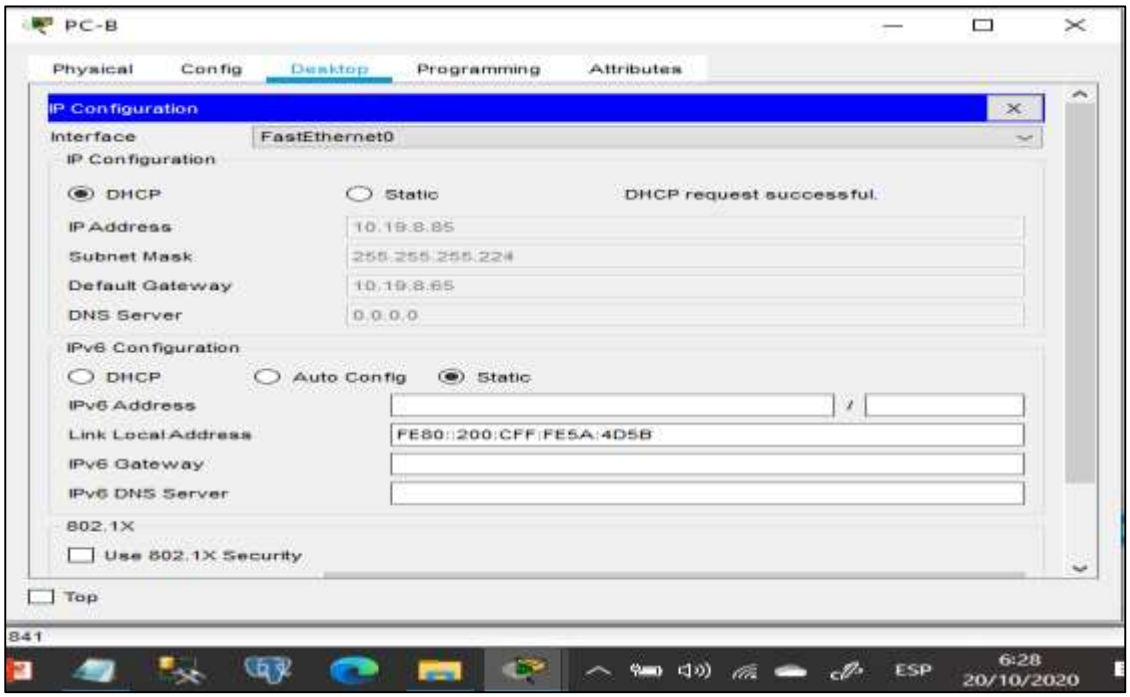


Fuente propia

Tabla 8. Detalle de configuración de red host PC-A

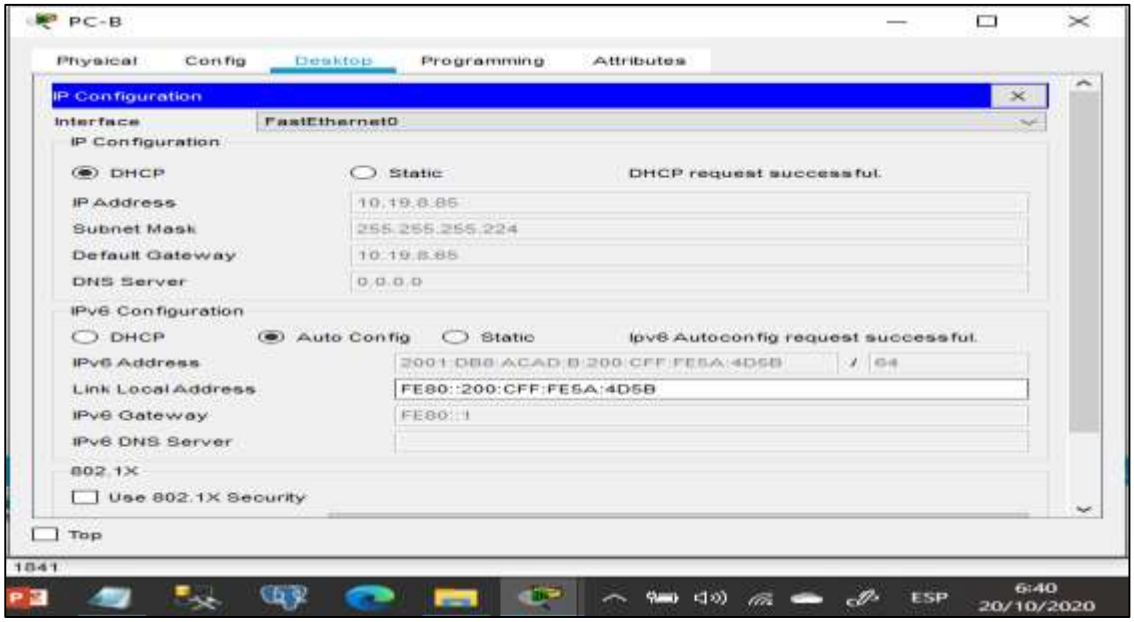
PC-A Network Configuration	
Descripción	
Dirección física	0001.97C7.6711
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 6. Verificación de Configuración DHCP host PC-B



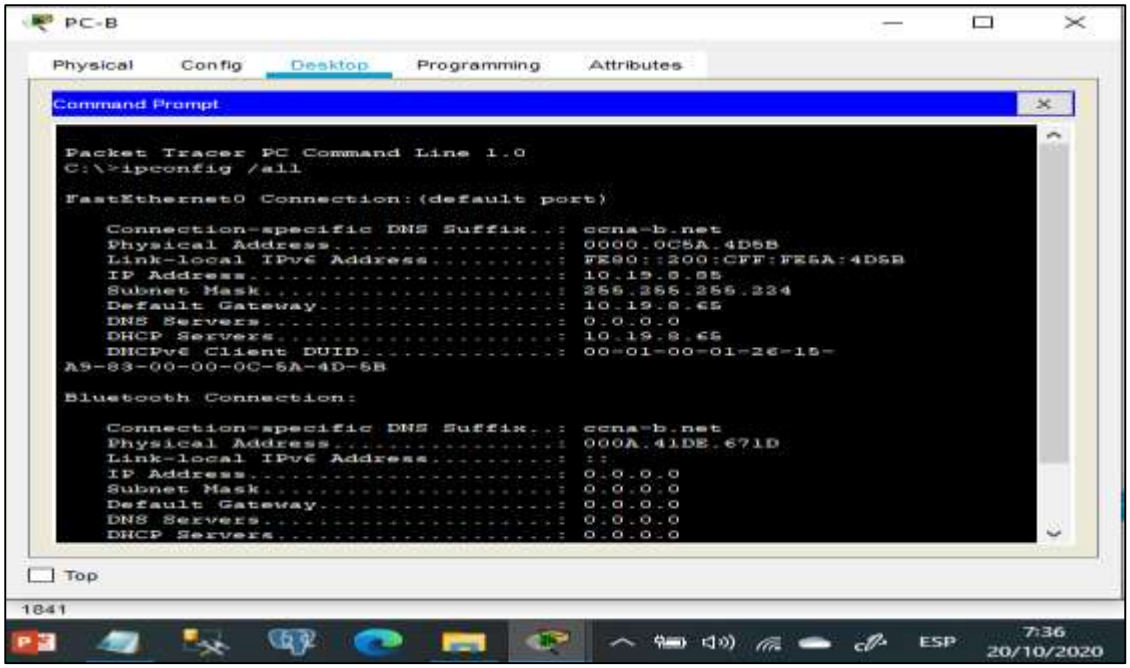
Fuente Propia

Figura 7.Asignación Estática de IPV6 y link Local PC-B



Fuente propia

Figura 8. Configuración de red host PC-B



Fuente propia

Tabla 9. Detalle de configuración de red host PC-B

PC-A Network Configuration	
Descripción	
Dirección física	0000.0C5A.4D5B
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

1.4 Probar y verificar la conectividad de extremo a extremo

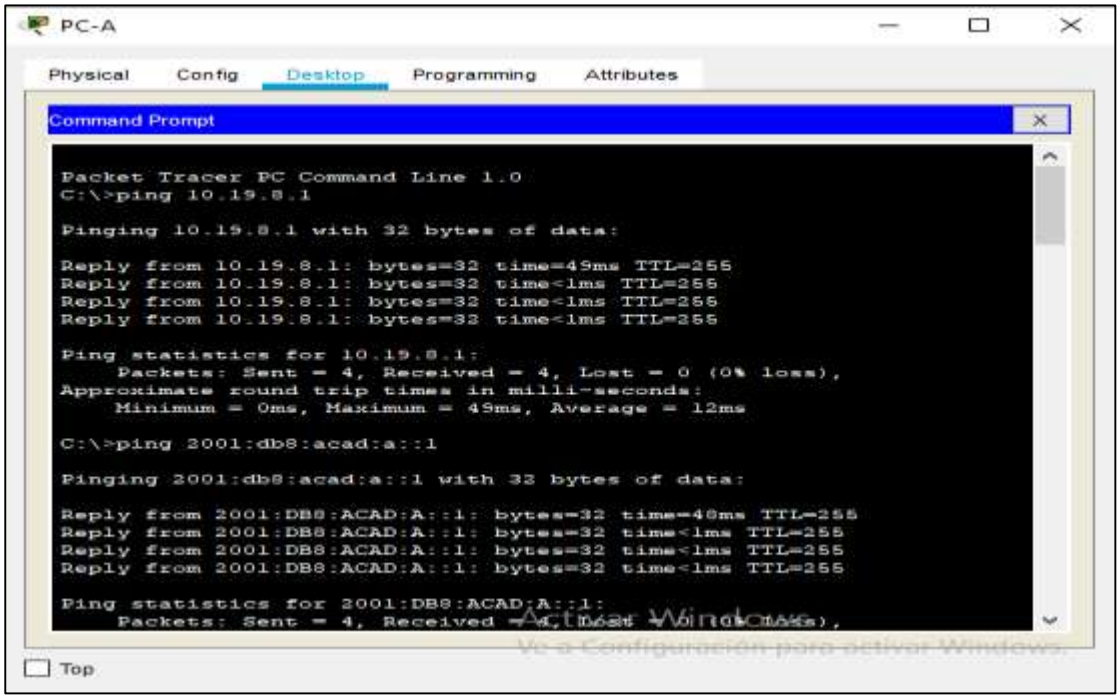
Haciendo uso del comando ping, se procede a probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red, según requerimientos y resultados detallados en la siguiente tabla.

Tabla 10. Verificación de Conectividad entre dispositivos

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	satisfactorio
		IPv6	2001:db8:acad:a: :1	satisfactorio
	R1, G0/0/1.3	Dirección	10.19.8.65	satisfactorio
		IPv6	2001:db8:acad:b::1	satisfactorio
	R1, G0/0/1.4	Dirección	10.19.8.97	satisfactorio
		IPv6	2001:db8:acad:c::1	satisfactorio
	S1, VLAN 4	Dirección	10.19.8.98	satisfactorio
		IPv6	2001:db8:acad:c::98	satisfactorio
	S2, VLAN 4	Dirección	10.19.8.99	satisfactorio
		IPv6	2001:db8:acad:c::99	satisfactorio
	PC-B	Dirección	10.19.8.86	satisfactorio
		IPv6	2001:db8:acad:b::50	satisfactorio
	R1 Bucle 0	Dirección	209.165.201.1	satisfactorio
		IPv6	2001:db8:acad:209: :1	satisfactorio
PC-B	R1 Bucle 0	Dirección	209.165.201.1	satisfactorio
		IPv6	2001:db8:acad:209::1	satisfactorio
	R1, G0/0/1.2	Dirección	10.19.8.1	satisfactorio
		IPv6	2001:db8:acad:a: :1	satisfactorio
	R1, G0/0/1.3	Dirección	10.19.8.65	satisfactorio
		IPv6	2001:db8:acad:b: :1	satisfactorio
	R1, G0/0/1.4	Dirección	10.19.8.97	satisfactorio

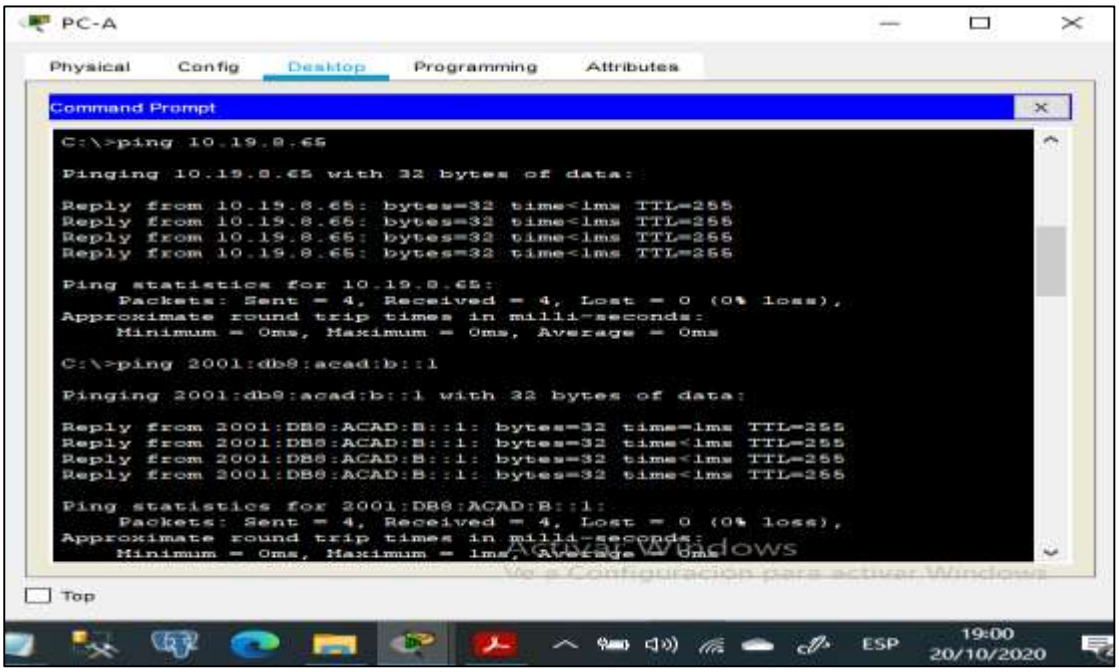
		IPv6	2001:db8:acad:c: :1	satisfactorio
	S1, VLAN 4	Dirección	10.19.8.98	satisfactorio
		IPv6	2001:db8:acad:c: :98	satisfactorio
	S2, VLAN 4	Dirección	10.19.8.99.	satisfactorio
		IPv6	2001:db8:acad:c: :99	satisfactorio

Figura 9. Ping desde PC-A a R1, G0/0/1.2



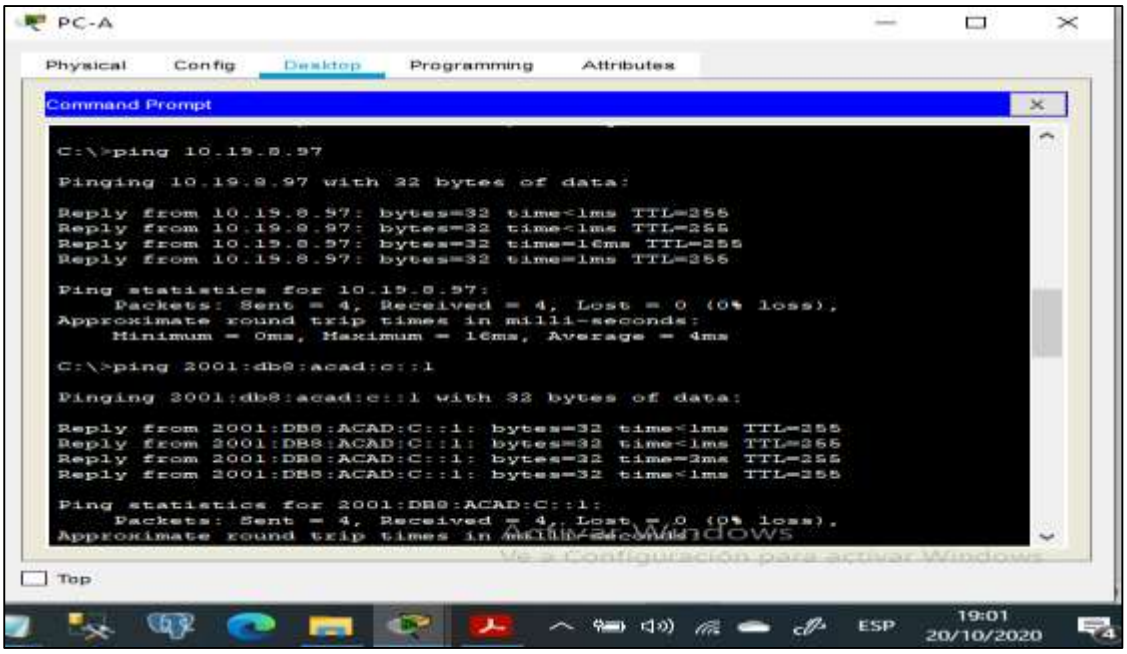
Fuente propia

Figura 10. Ping desde PC-A a *R1,* G0/0/1.3



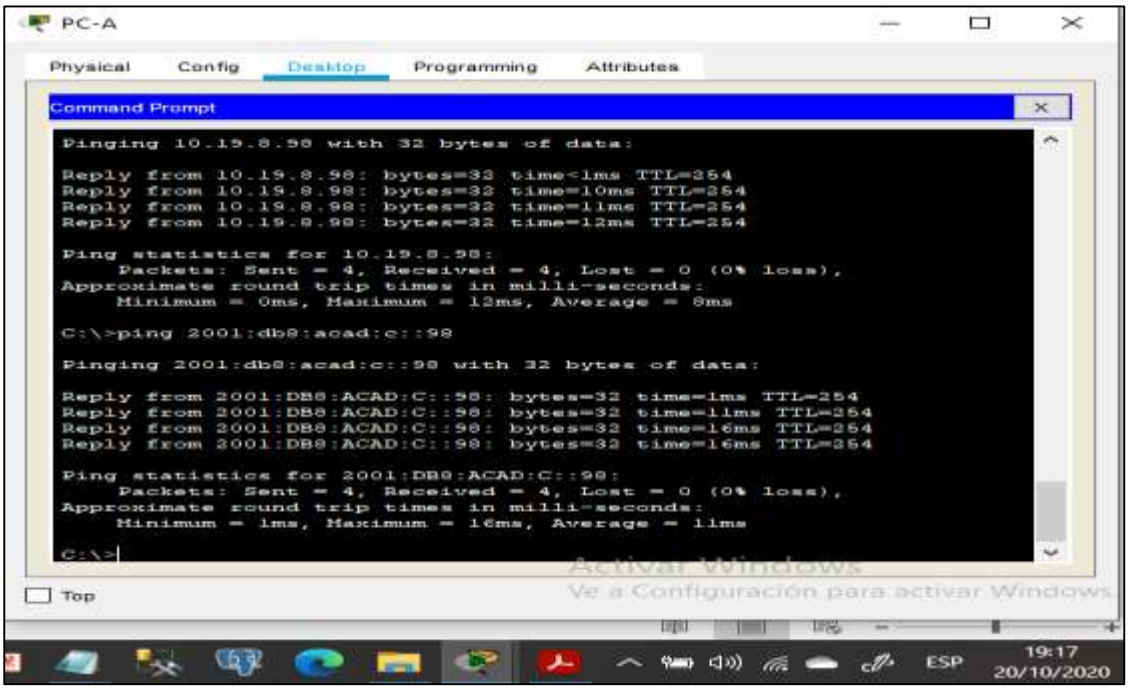
Fuente propia

Figura 11. Ping desde PC-A a R1, G0/0/1.4



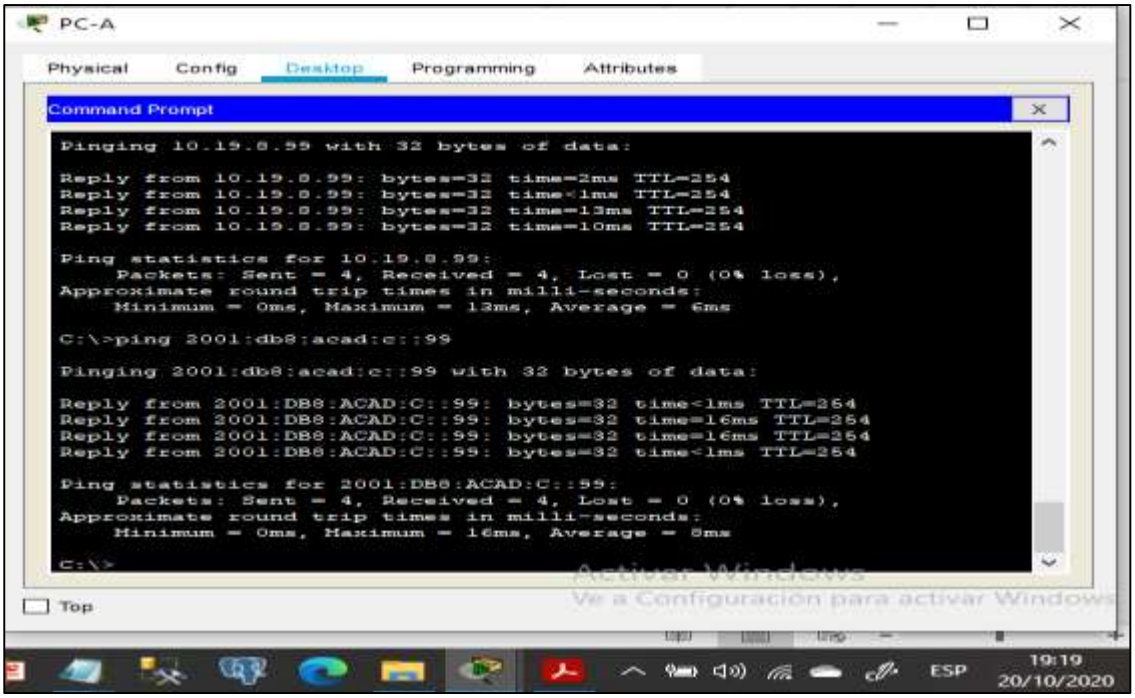
Fuente propia

Figura 12. Ping desde PC-A a S1, VLAN 4



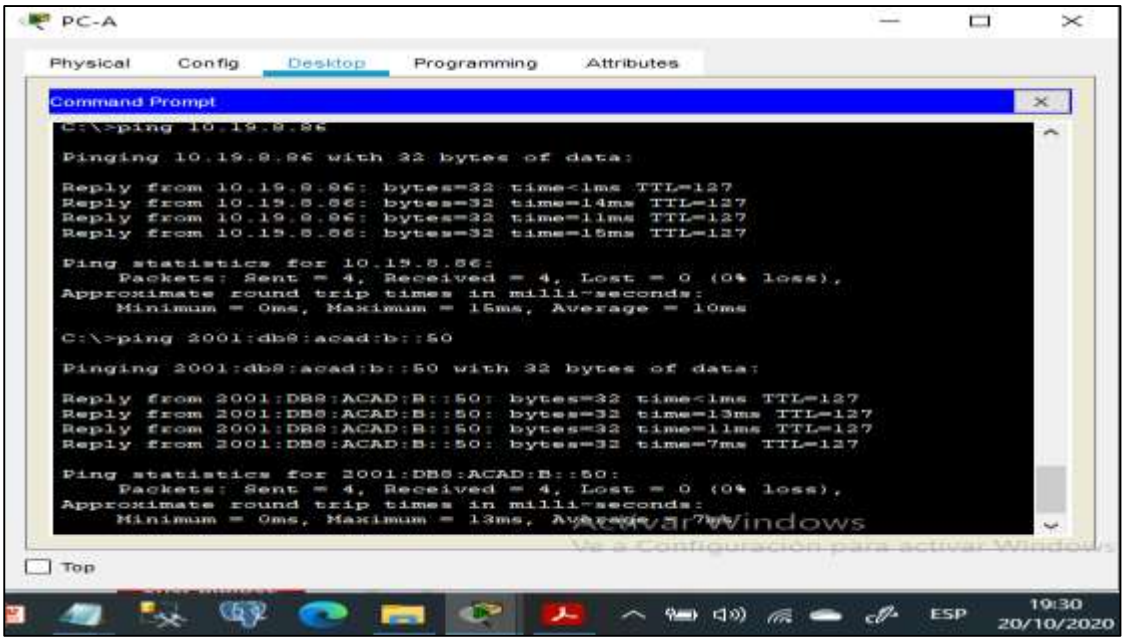
Fuente propia

Figura 13. Ping desde PC-A a S2, VLAN 4



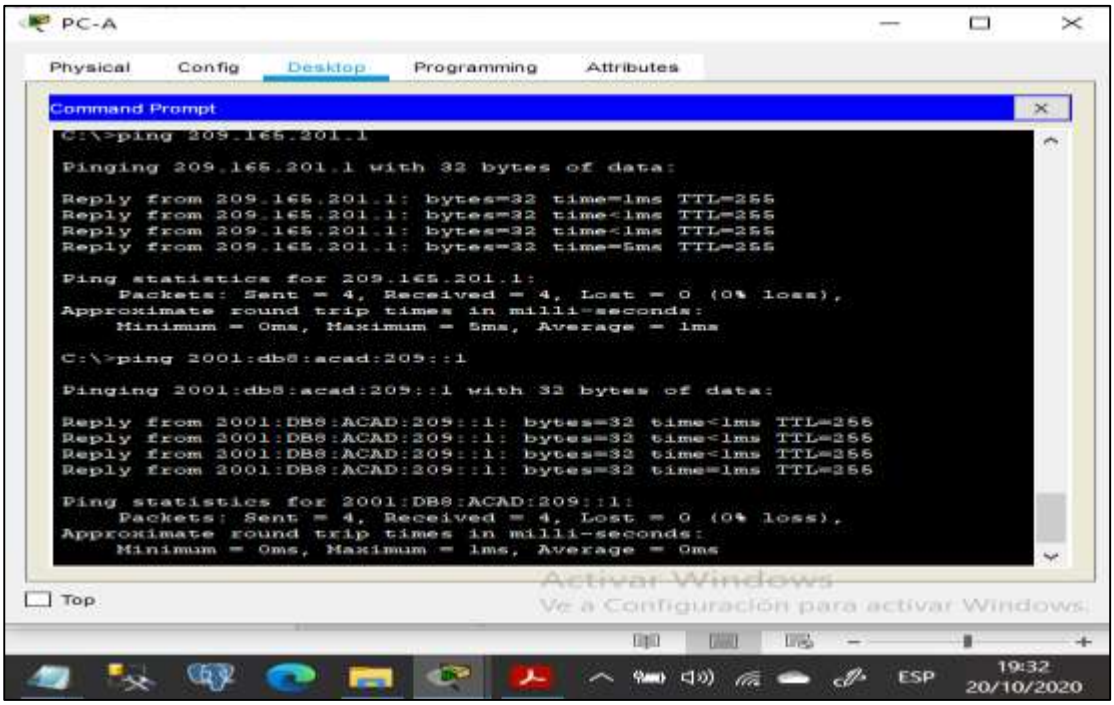
Fuente propia

Figura 14. Ping desde PC-A a PC-B



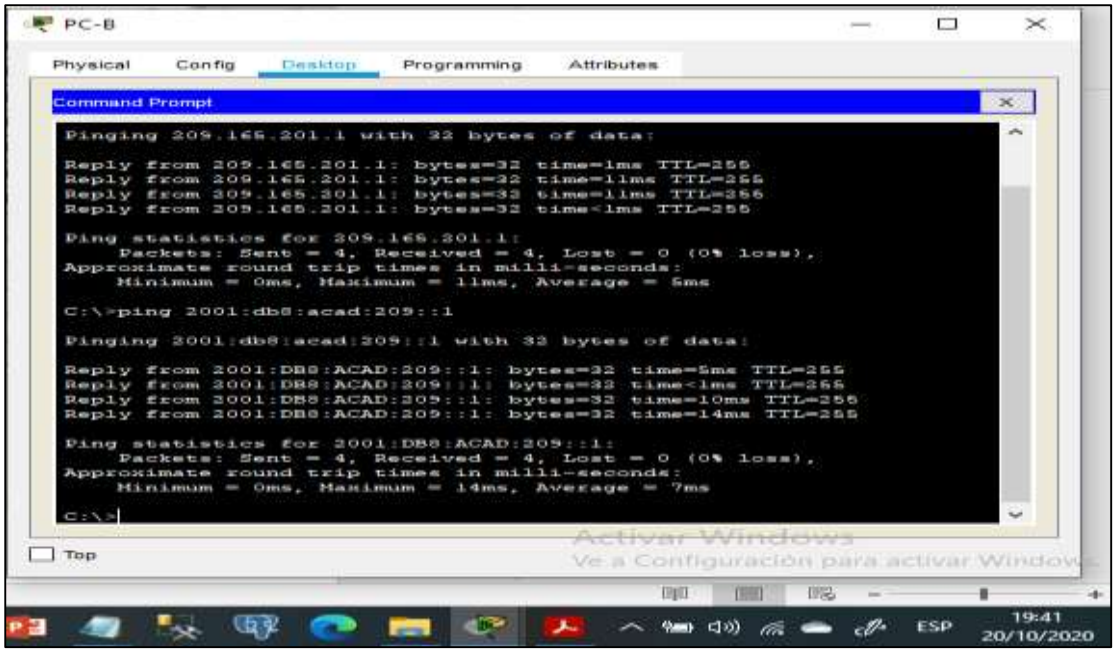
Fuente propia

Figura 15. Ping desde PC-A a R1, Bucle 0



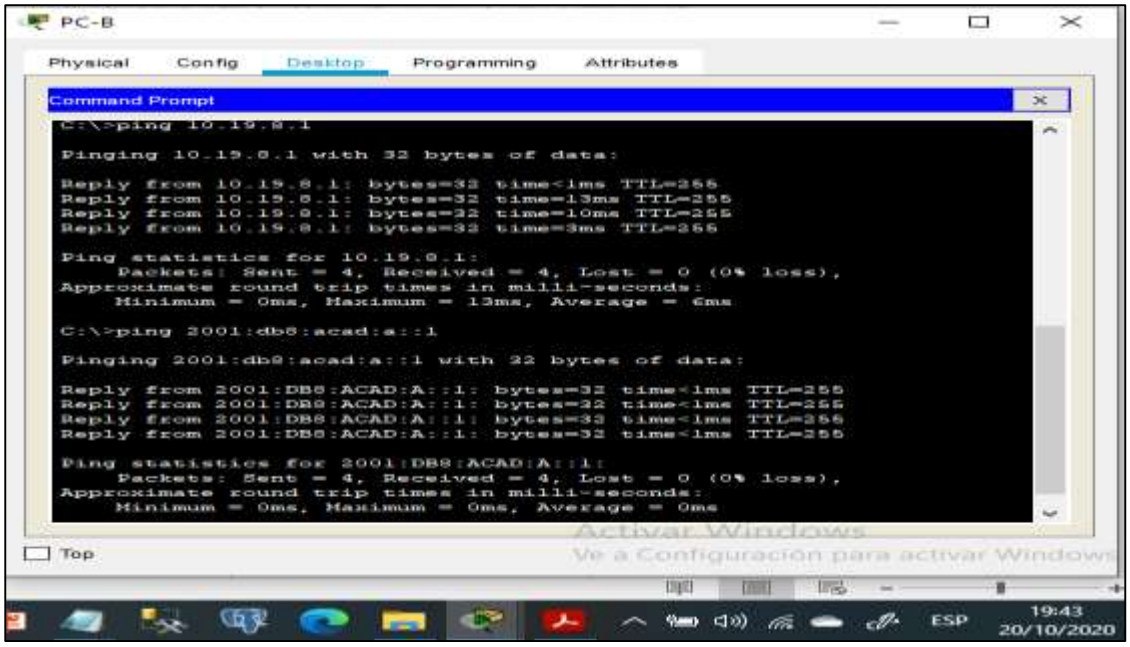
Fuente propia

Figura 16. Ping desde PC-B a R1, Bucle 0



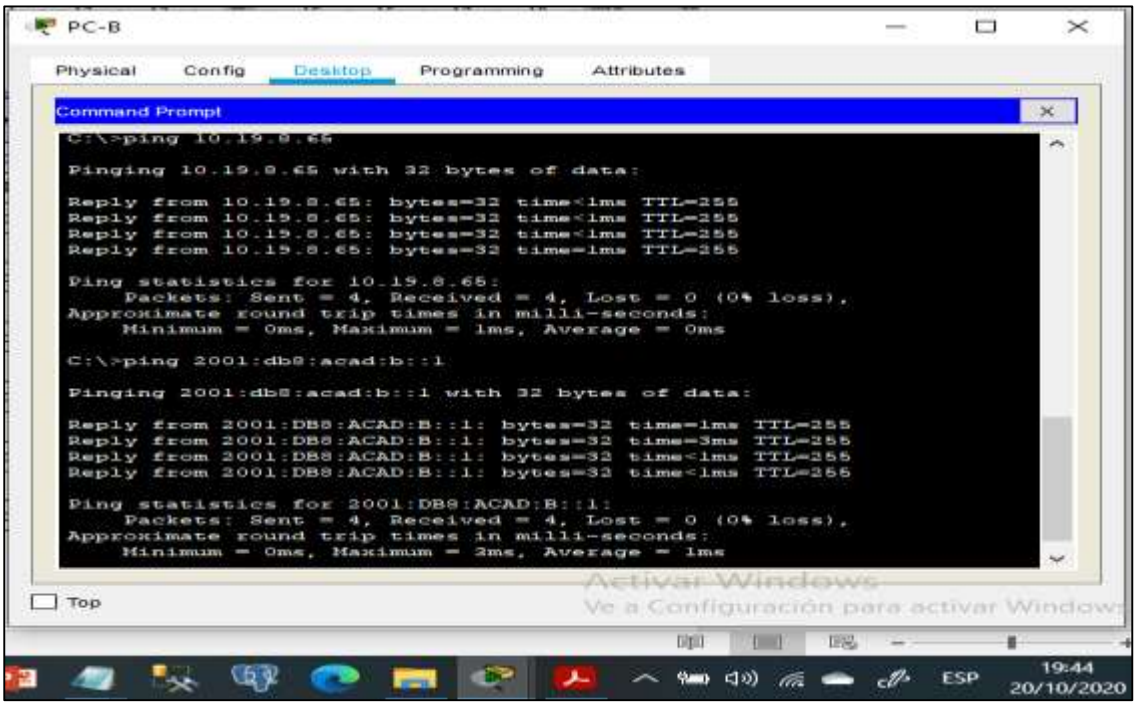
Fuente propia

Figura 17. Ping desde PC-B a R1, G0/0/1.2



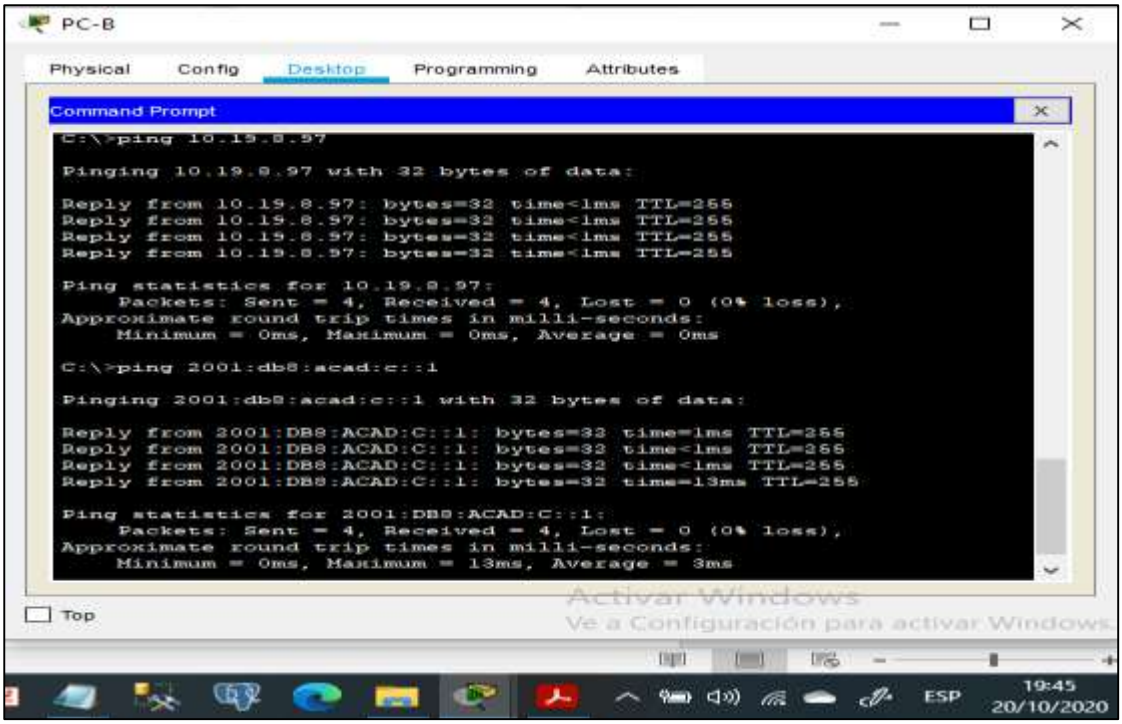
Fuente propia

Figura 18. Ping desde PC-B a R1, G0/0/1.3



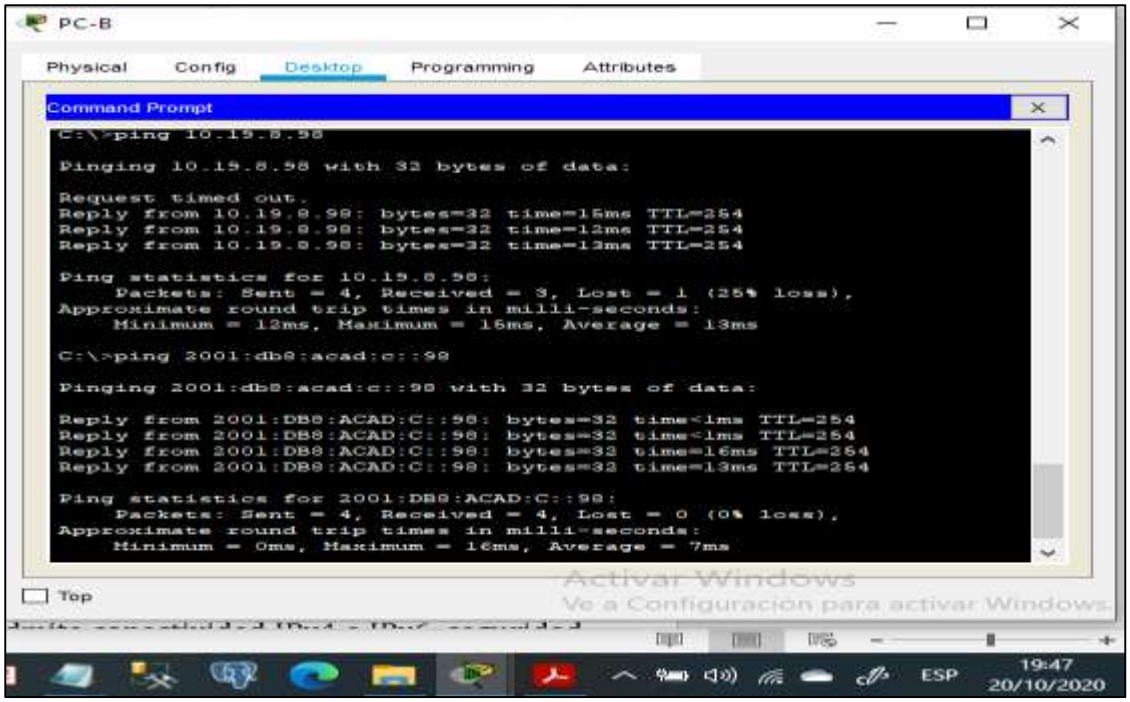
Fuente propia

Figura 19. Ping desde PC-B a R1, G0/0/1.4



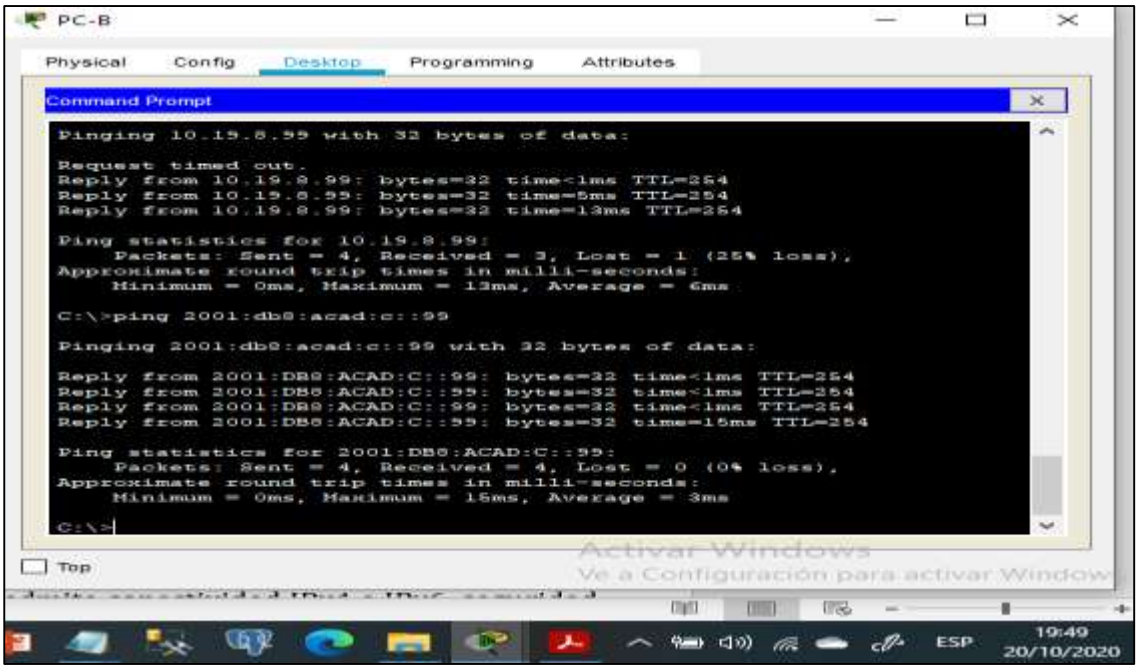
Fuente propia

Figura 20. Ping desde PC-B a S1, VLAN 4



Fuente propia

Figura 21. Ping desde PC-B a S2, VLAN 4

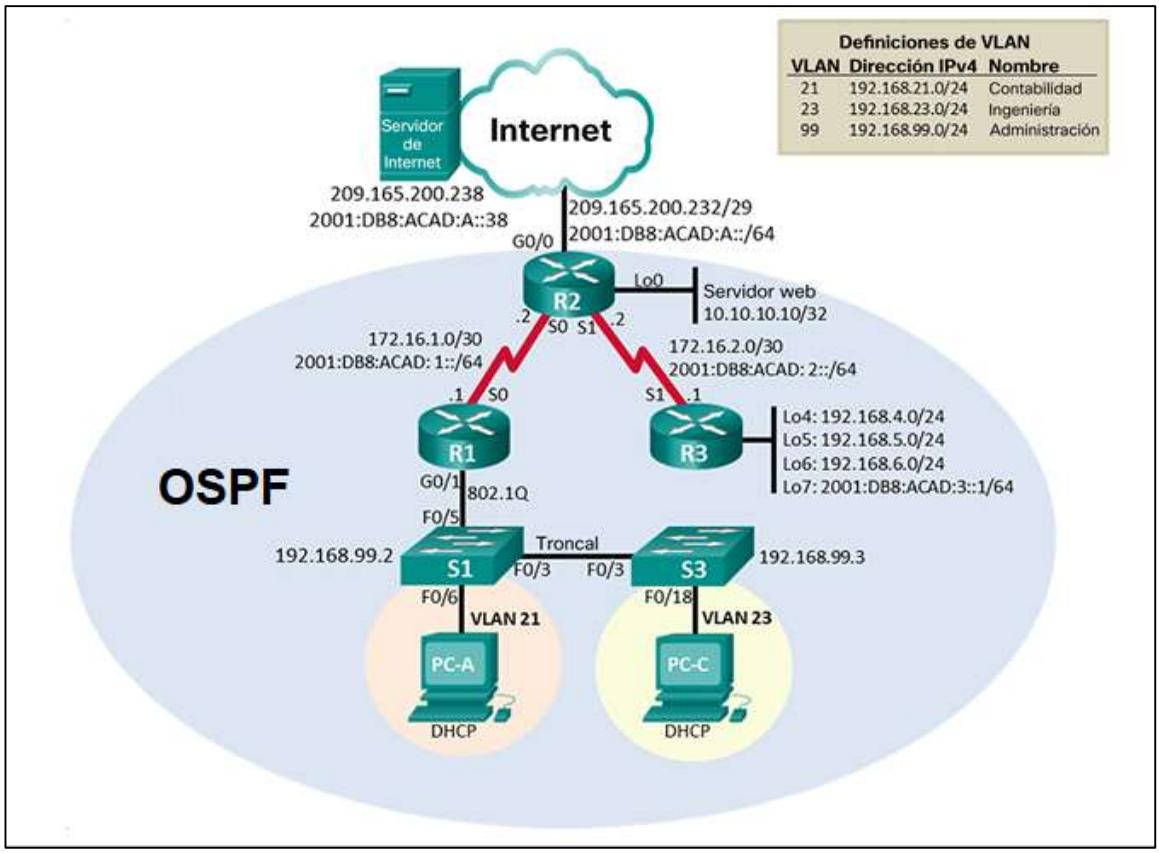


Fuente propia

2 Desarrollo del escenario 2

Topología

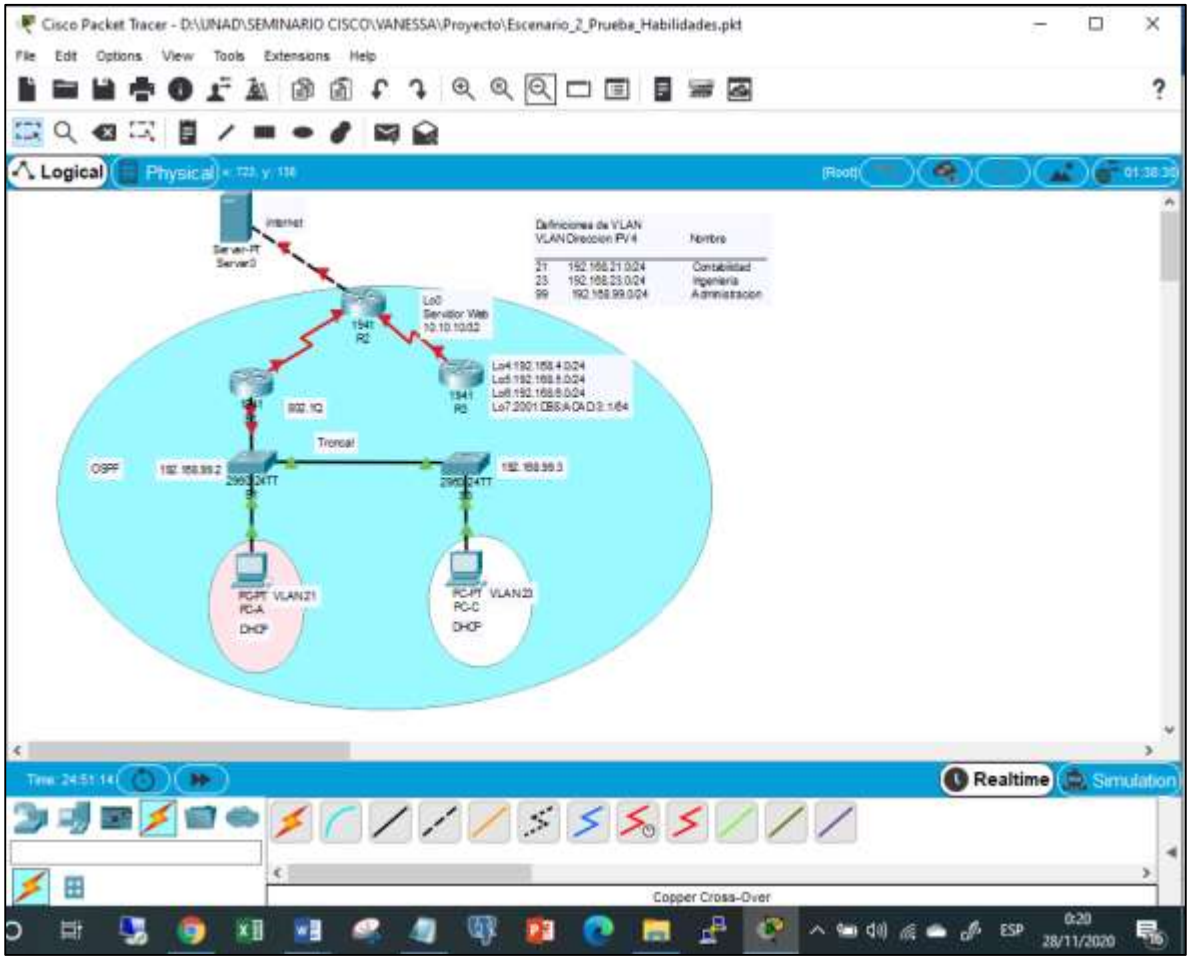
Figura 22. Topología de Red Escenario 2



Prueba de habilidades CCNA II-2020

Conforme al planteamiento del escenario 2, se procede a realizar la configuración física de 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.

Figura 23. Topología de red Escenario 2



Fuente propia

2.1 Inicializar dispositivos

2.1.1 Inicializar y volver a cargar los routers y los switches

Como primer paso, se procede a borrar las configuraciones de inicio en cada uno de los routers y de los switches, así como la eliminación de las bases de datos de las VLAN en los switches y se vuelven a cargar los dispositivos, verificando con el mensaje arrojado por los dispositivos que no tienen configuración de inicio. Estas tareas se llevan a cabo mediante el uso de los comandos descritos en la siguiente tabla.

Tabla 11.Borrado de Configuración inicial Routers y Switches

Tarea	Comando
Borrar las configuraciones de inicio en el Routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Borrar las configuraciones de inicio en los Switches y eliminación la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash Directory of flash:/ 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin 1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin

2.2 Configuración de los parámetros básicos de los dispositivos

Posterior a la inicialización de los dispositivos, se procede a realizar la configuración según el direccionamiento IP propuesto en la topología de red, iniciando por el Servidor de Internet, los Routers, Switches y PCs.

2.2.1 Configuración de la computadora de Internet

Tabla 12. Configuración de 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:A::1

2.2.2 Configuración de R1

Posteriormente se realiza la configuración básica de seguridad de R1, que incluye las siguientes tareas: Desactivación de la búsqueda de DNS, Nombre del router, contraseñas de exec privilegiado, acceso a consola y acceso Telnet, mensaje de advertencia de prohibido el acceso no autorizado, configuración de la interfaz s0/0/0 y las rutas predeterminadas.

Tabla 13. Configuración Básica de R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#config t 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 # UnAuthorized Access is prohibite!#

Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#description connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

2.2.3 Configuración de R2

Ahora procedemos con la configuración básica de seguridad de R2, que incluye las siguientes tareas: Desactivación de la búsqueda de DNS, Nombre del router, contraseñas de exec privilegiado, acceso a consola y acceso Telnet, Habilitar el servidor HTTP, mensaje de advertencia de prohibido el acceso no autorizado, configuración de las interfaces s0/0/0, S0/0/1, G0/0, loopback 0 y las rutas predeterminadas.

Tabla 14. Configuración Básica de R2.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable 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 (Comando no soportado por Packet Tracer)
Mensaje MOTD	R2(config)#banner motd # UnAuthorized Access is prohibite!#
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config-if)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown

Interfaz loopback 0 (servidor web simulado)	R2(config)#int l0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description simulated web server R2(config-if)#exit
Ruta predeterminada	R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config-if)#ipv6 route ::/0 g0/0

2.2.4 Configuración de R3

Se procede con la configuración básica de seguridad de R3, que incluye las siguientes tareas: Desactivación de la búsqueda de DNS, Nombre del router, contraseñas de exec privilegiado, acceso a consola y acceso Telnet, mensaje de advertencia de prohibido el acceso no autorizado, configuración de las interfaces S0/0/1, loopback 4, loopback 5, loopback 6, loopback 7 y las rutas predeterminadas.

Tabla 15.Configuración Básica de R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable 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
Contraseña de acceso a la consola	R3(config)#line console 0 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 # UnAuthorized Access is prohibite!#
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#description connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#Int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#Int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#Int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#Int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

2.2.5 Configuración de S1

Se procede con la configuración básica de seguridad de S1, que incluye las siguientes tareas: Desactivación de la búsqueda de DNS, Nombre del Switch, contraseñas de exec privilegiado, acceso a consola y acceso Telnet y mensaje de advertencia de prohibido el acceso no autorizado.

Tabla 16. Configuración Básica de S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t 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 # UnAuthorized Access is prohibite!#

2.2.6 Configuración de S3

Se procede con la configuración básica de seguridad de S3, que incluye las siguientes tareas: Desactivación de la búsqueda de DNS, Nombre del Switch, contraseñas de exec privilegiado, acceso a consola y acceso Telnet y mensaje de advertencia de prohibido el acceso no autorizado.

Tabla 17. Configuración Básica de S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t 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-line)#banner motd # UnAuthorized Access is prohibite!#

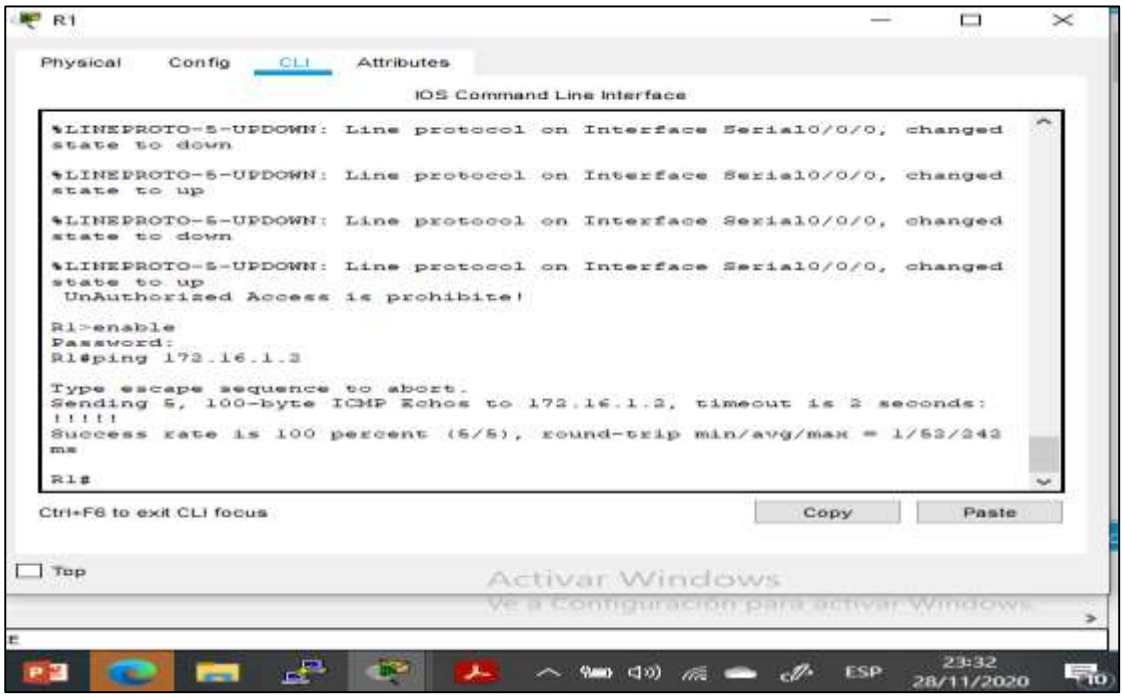
2.2.7 Verificación de conectividad de la red.

Utilizando el comando ping probamos la conectividad entre los dispositivos de red. En la siguiente tabla se evidencian el origen y destino de los dispositivos y los resultados obtenidos en cada uno de ellos:

Tabla 18. conectividad entre R1, R2 y Servidor

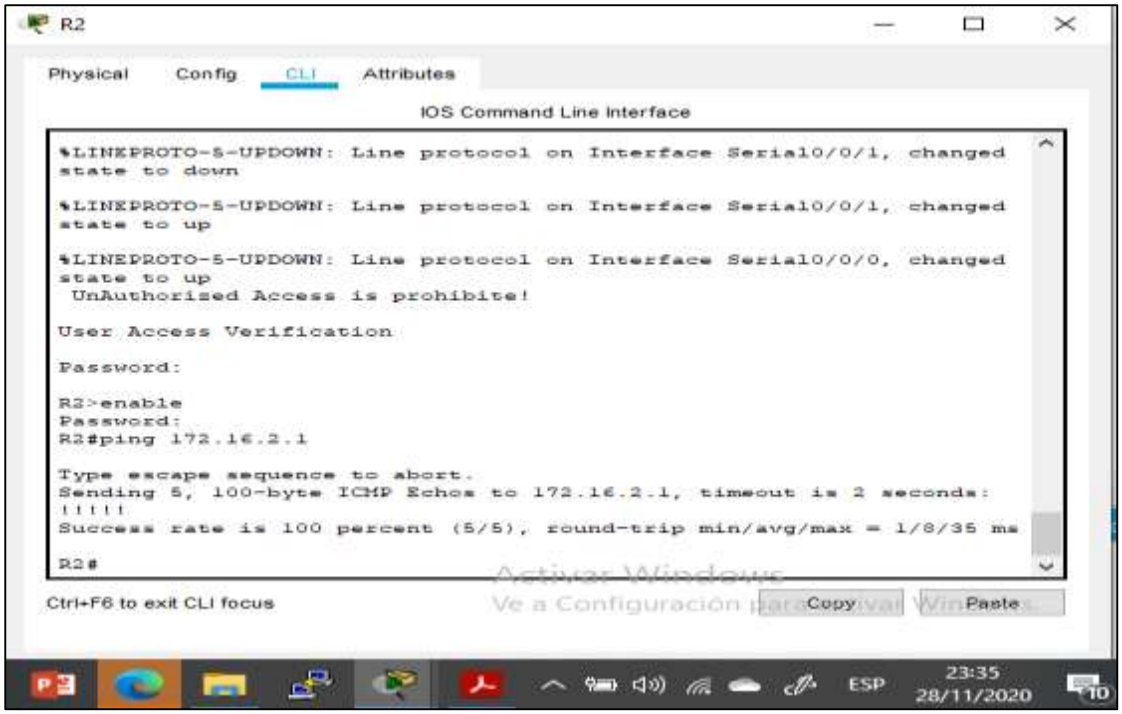
Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	Satisfactorio
R2	R3, S0/0/1	172.16.2.1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.233	Satisfactorio

Figura 24. Ping desde R1 a R2, S0/0/0



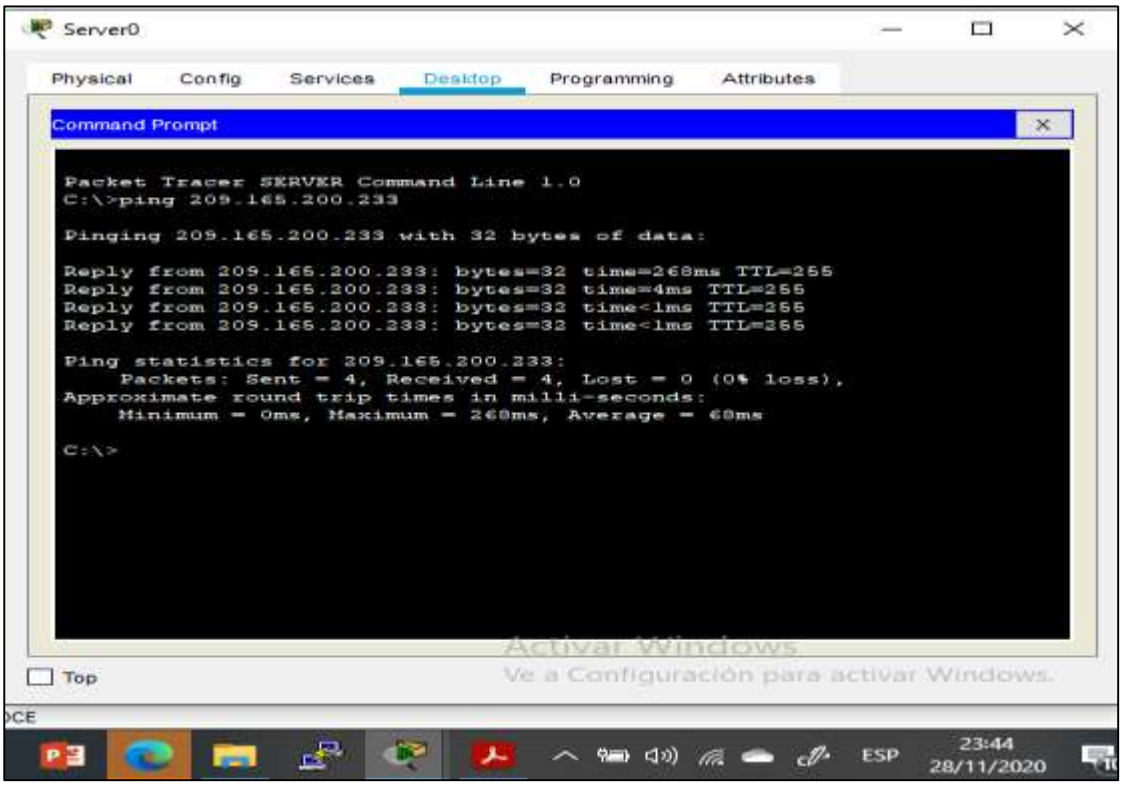
Fuente Propia

Figura 25. . Ping desde R2 a R3, S0/0/1



Fuente Propia

Figura 26. Ping de PC de Internet a puerta de enlace



Fuente Propia

2.3 Configuración de Seguridad de los Switch, las VLAN y el routing entre VLAN

Conforme a la tabla de equivalencias de VLAN propuesta para la topología de red, se realiza la creación y nombramiento de cada una de las VLAN 21(Contabilidad), 23(Ingeniería) y 99(Administración). Igualmente, la asignación de la dirección IP de administración, configuración de la primera dirección IPv4 de la subred como el Gateway predeterminado, Configuración de los puertos troncales y Configuración de los puertos de acceso y seguridad, finalmente apagado de los puertos sin uso.

2.3.1 Configuración de Seguridad en S1.

Tabla 19. Configuración de Seguridad en S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1>enable S1#config t 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

2.3.2 Configuración de Seguridad en S3.

Tabla 20. Configuración de Seguridad en S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S3>enable S3#config t 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)#int vlan 99 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 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
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

2.3.3 Configuración de VLAN de R1

En R1, Se realiza la configuración de las subinterfaces en G0/1: 802.1Q .21 asignando la primera dirección disponible a la VLAN 21, LAN de Contabilidad, 802.1Q .23 asignando la primera dirección disponible a la VLAN 23, LAN de Ingeniería, 802.1Q .99 asignando la primera dirección disponible a la VLAN 99, LAN de Administración y se procede a activar la interfaz G0/1.

Tabla 21. Configuración de VLAN de R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#configure terminal R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#int g0/1 R1(config-if)#no shutdown

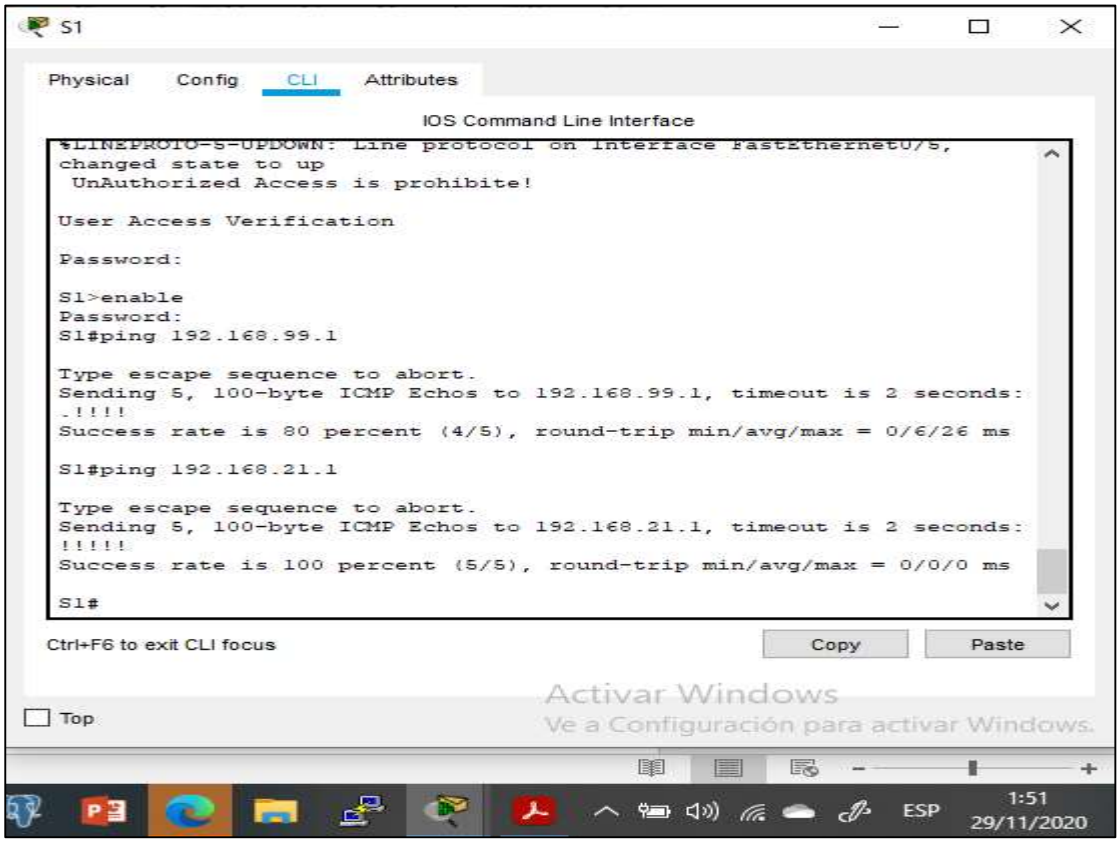
2.3.4 Verificación de conectividad en la R1

Utilizamos el comando ping para probar la conectividad entre los switches y el R1. En la siguiente tabla se detallan los orígenes y destinos y los resultados obtenidos.

Tabla 22. Conectividad entre los switches y el R1

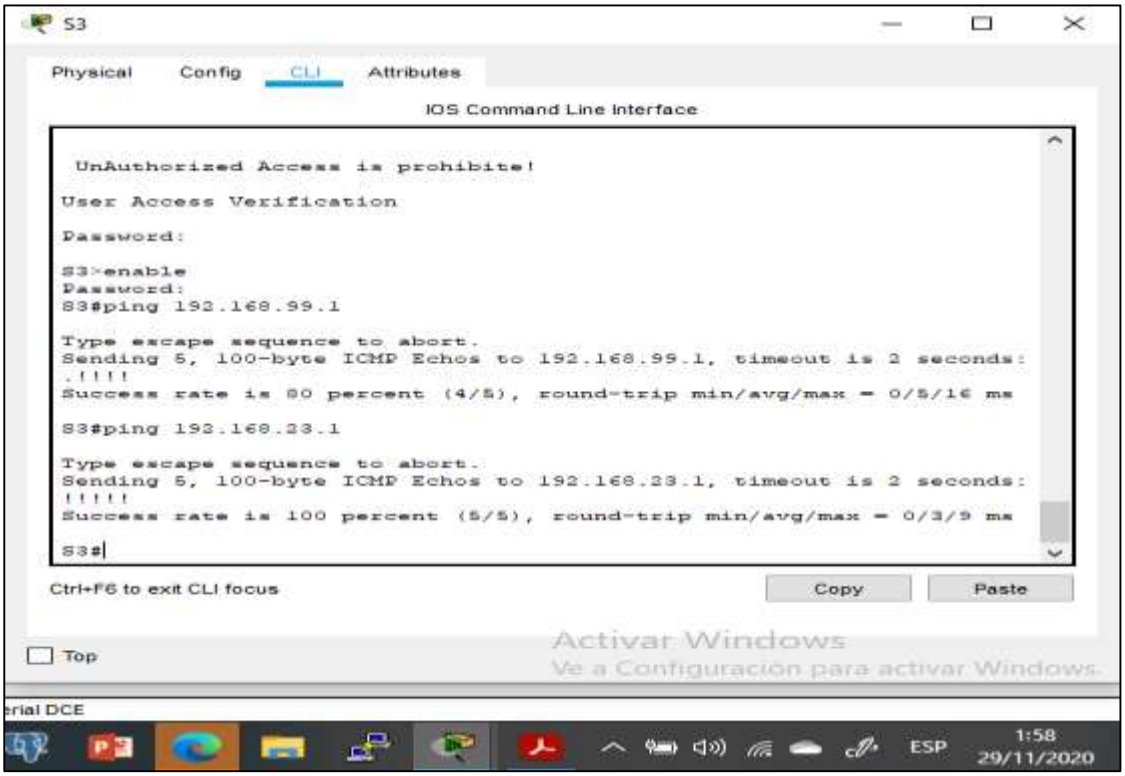
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.1	Satisfactorio

Figura 27. Ping de S1 a R1 VLAN 21 y VLAN 99



Fuente Propia

Figura 28. Ping de S3 a R1 VLAN 21 y VLAN 99



Fuente Propia

2.4 Configuración del protocolo routing dinámico OSPF

2.4.1 Configuración OSPF en R1

Tabla 23. Configuración OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1

Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

2.4.2 Configuración OSPF en R2

Tabla 24.Configuración OSPF en R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0

Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	

2.4.3 Configuración OSPF en R3

Tabla 25. Configuración OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
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

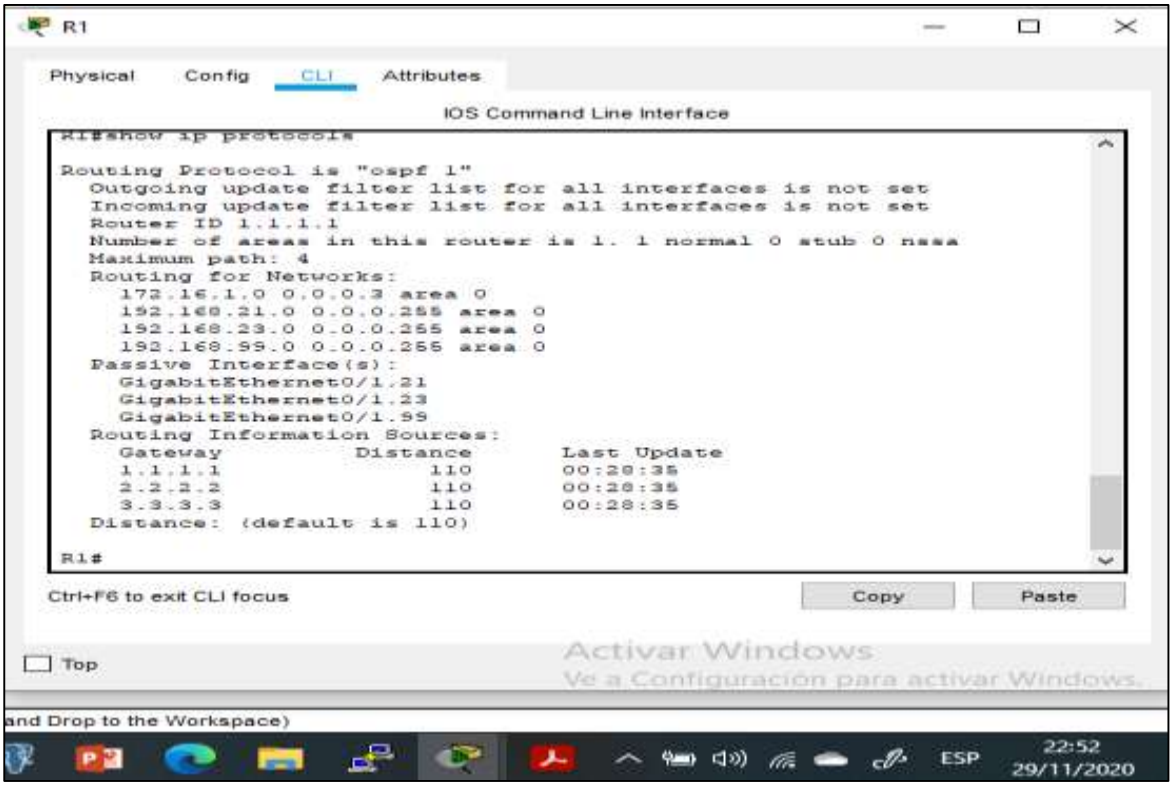
2.4.4 Verificación de la información de OSPF

Posterior a la configuración del protocolo OSPF en cada uno de los routers, procedemos a verificar con los comandos relacionados en la siguiente tabla, que la configuración sea exitosa.

Tabla 26. Verificación de configuración OSPF

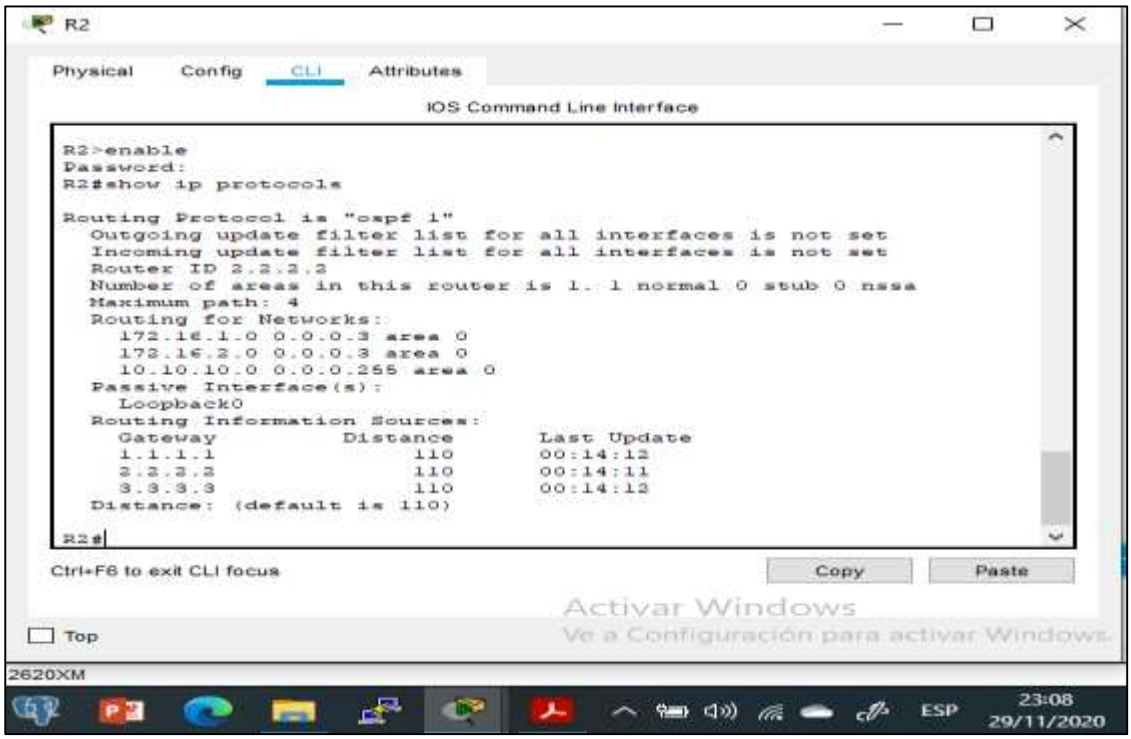
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración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

Figura 29. Verificación de configuración OSPF en R1

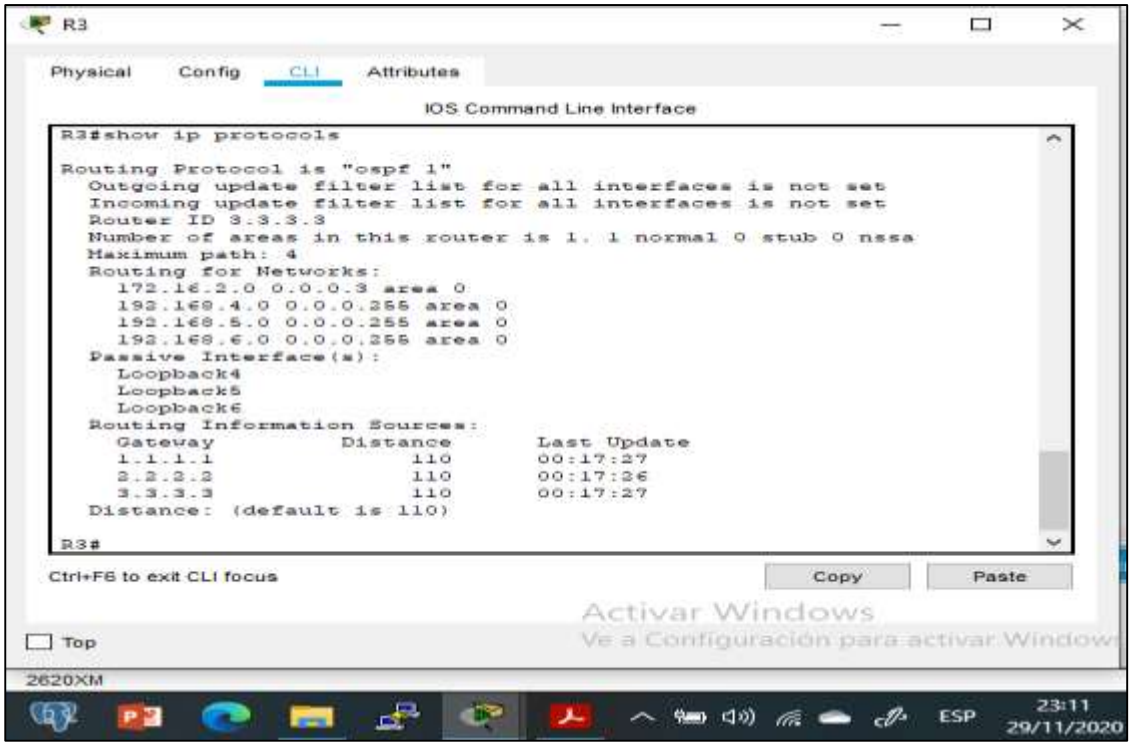


Fuente Propia

Figura 30. Verificación de configuración OSPF en R2

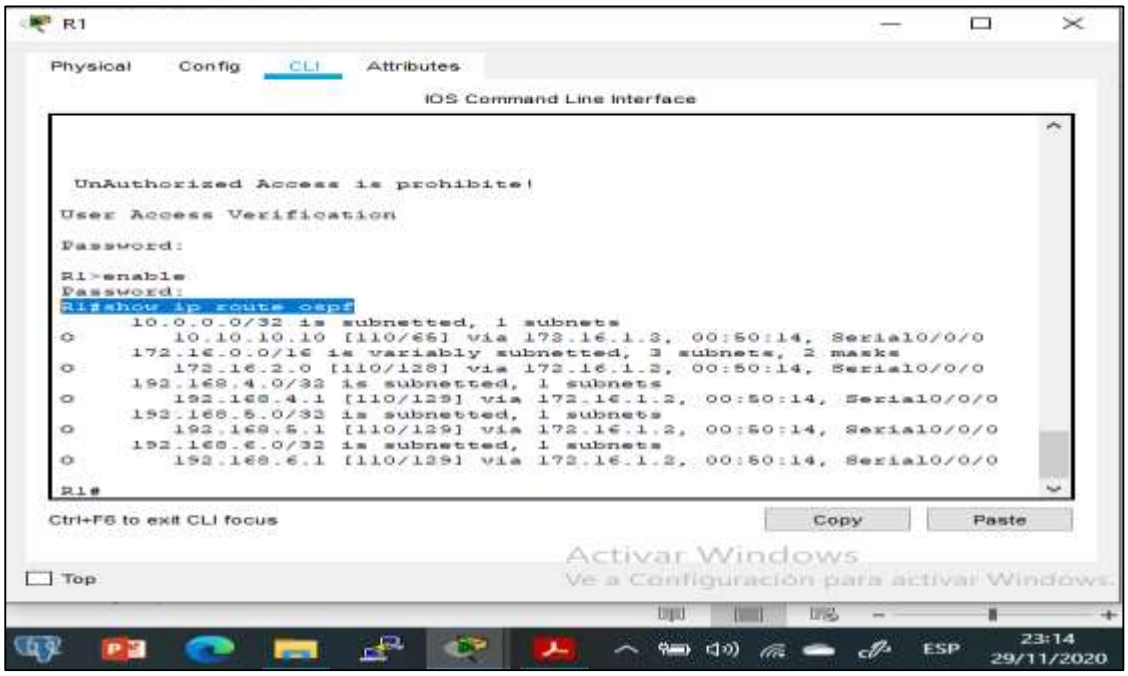


Fuente Propia



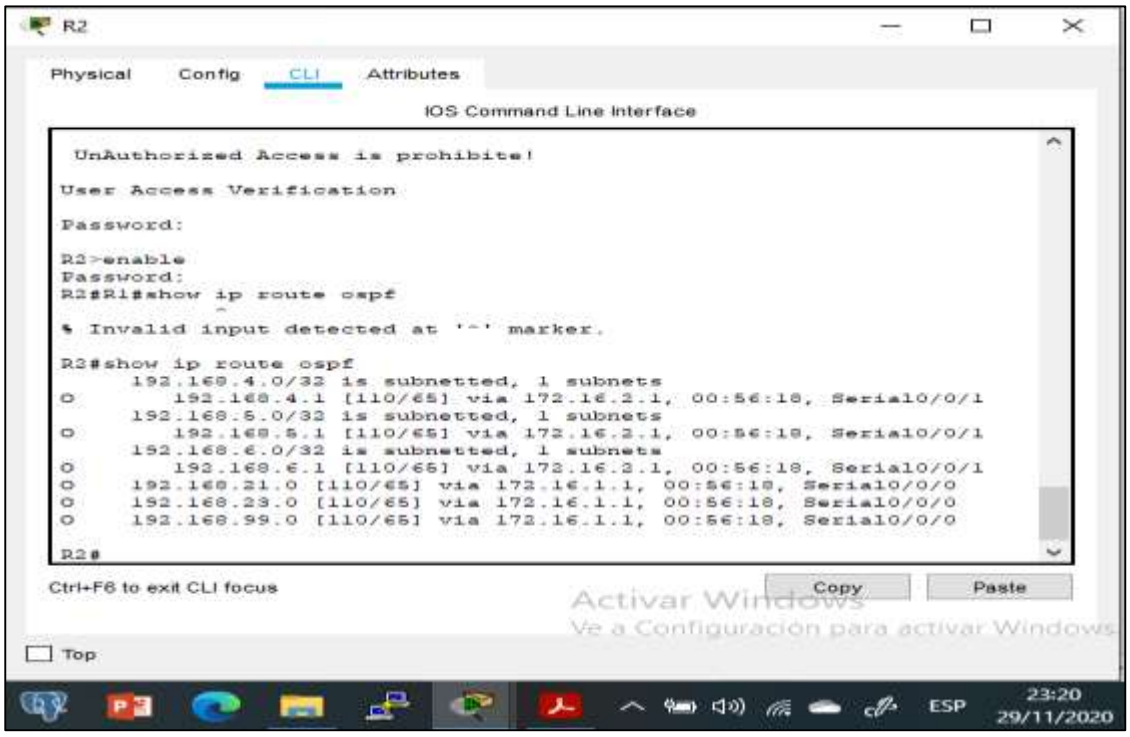
Fuente Propia

Figura 31. Verificación de rutas OSPF en R1



Fuente Propia

Figura 32.Verificación de rutas OSPF en R2



Fuente Propia

Figura 33. Verificación de rutas OSPF en R3

Fuente Propia

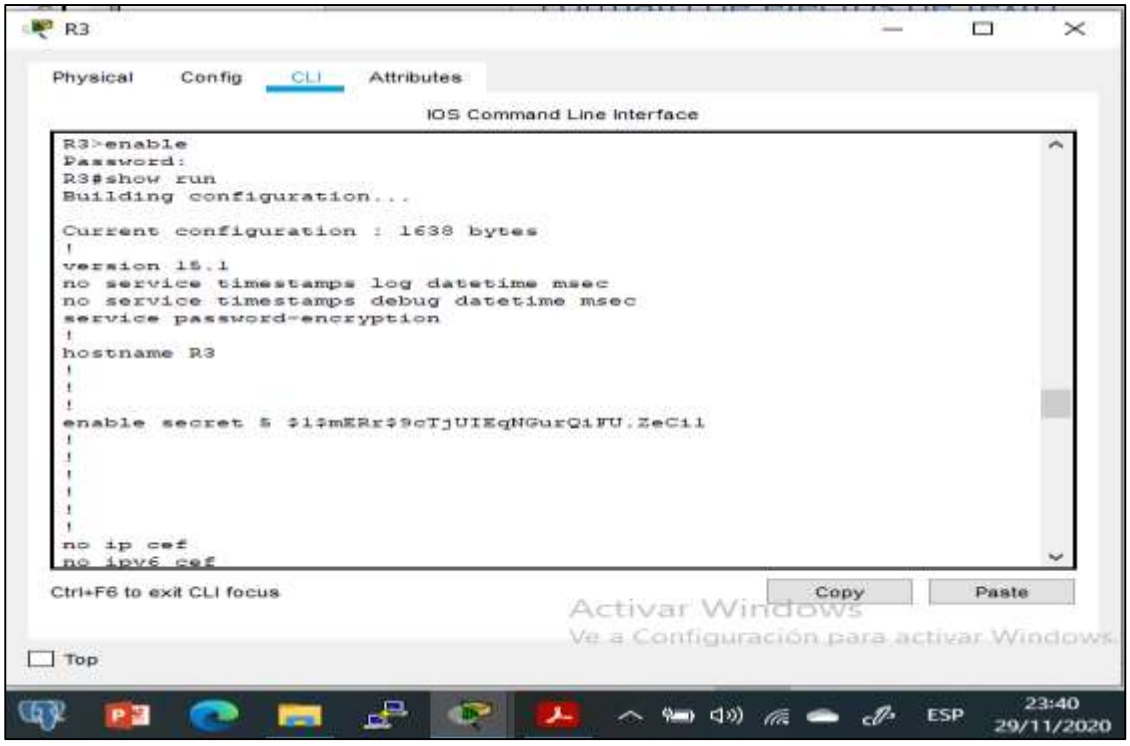
Figura 34. Verificación de sección de OSPF ejecución en R1

Fuente Propia

Figura 35. Verificación de sección de OSPF ejecución en R2

Fuente Propia

Figura 36.Verificación de sección de OSPF ejecución en R3



Fuente Propia

2.5 Implementación de DHCP y NAT para IPv4

2.5.1 Configuración de R1 como servidor de DHCP para las VLAN 21 y 23

Procedemos a realizar la configuración de R1 como servidor de DHCP para las VLAN 21 y 23, reservando las primeras 20 direcciones IP para configuraciones estáticas respectivamente. Igualmente se crea el pool DHCP para las VLAN.

Tabla 27. Configuración de R1 como servidor de DHCP

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT R3(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)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com

2.5.2 Configuración de la NAT estática y dinámica en el R2

Se realiza la configuración de la NAT estática y dinámica en R2, para lo cual procedemos a crear una base de datos local con una cuenta de usuario, habilitando el servidor HTTP, creando una NAT estática al servidor web y configurando una ACL privada y definiendo el pool de direcciones IP públicas utilizables.

Tabla 28. Configuración de 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>enable R2#config t R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (comando no soportado en Packet Tracer)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (comando no soportado en Packet Tracer)
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
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

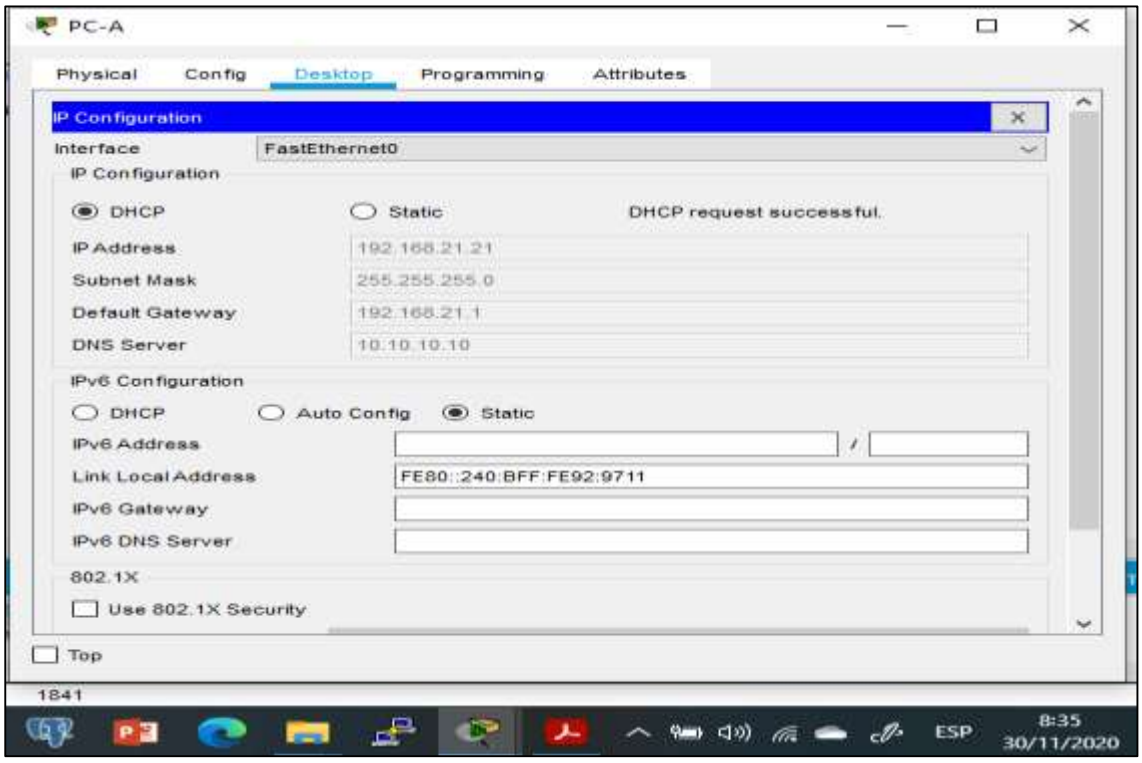
2.5.2 Verificación del protocolo DHCP y la NAT estática

Procedemos a verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta en los PC-A y PC-C para lo cual realizamos inicialmente la verificación físicamente en los PC. Posteriormente a través de la ejecución del comando ping comprobamos la conectividad entre los dispositivos. Los resultados obtenidos se detallan en la siguiente tabla y las imágenes.

Tabla 29.Verificación del protocolo DHCP y la NAT estática en los PC

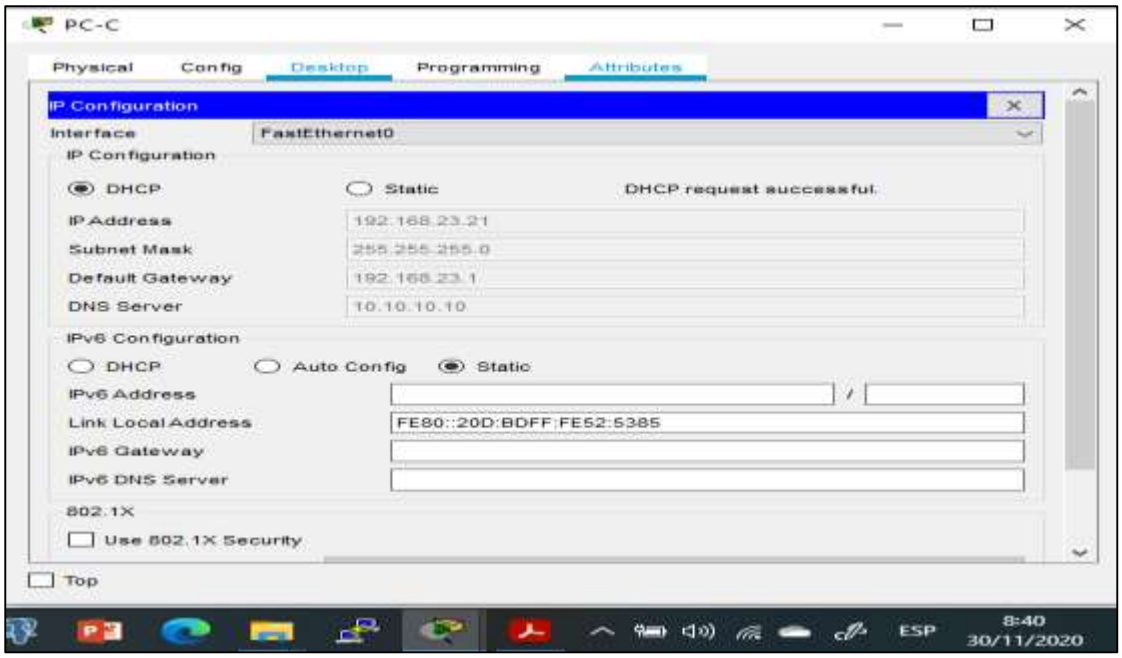
Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C	Satisfactorio
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet Tracert no soporta este procedimiento, dado que no acepto el comando ip http server

Figura 37. Verificación del protocolo DHCP en PC-A



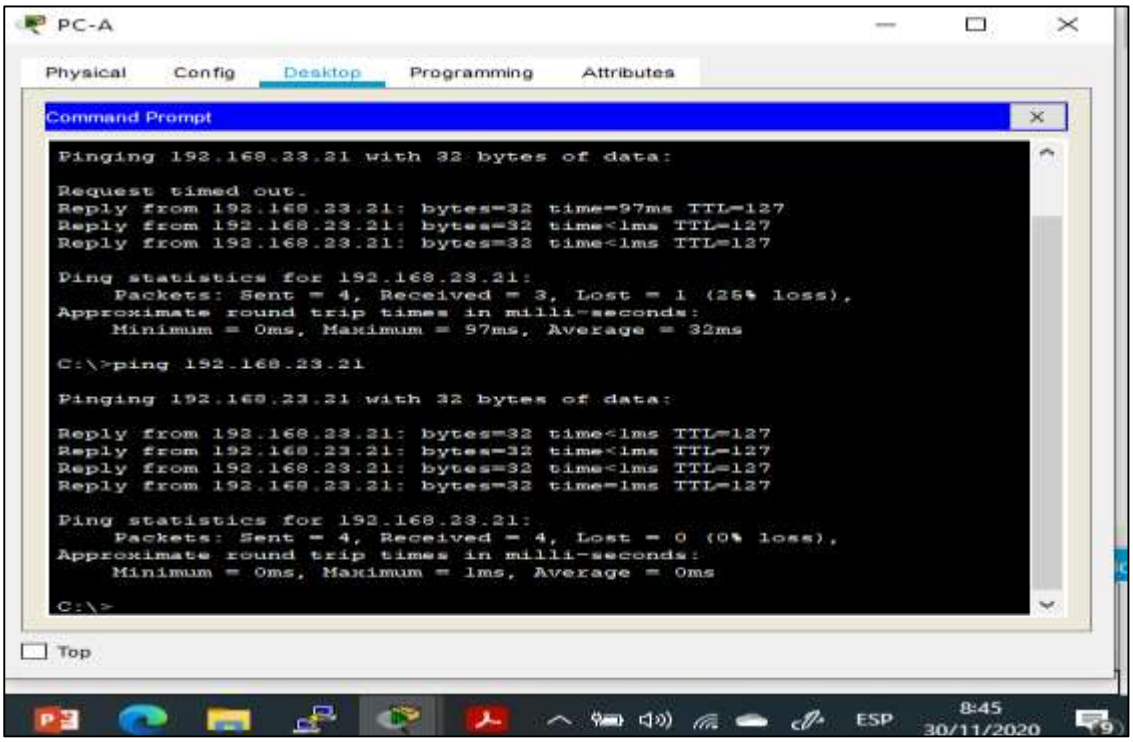
Fuente Propia

Figura 38. Verificación del protocolo DHCP en PC-C



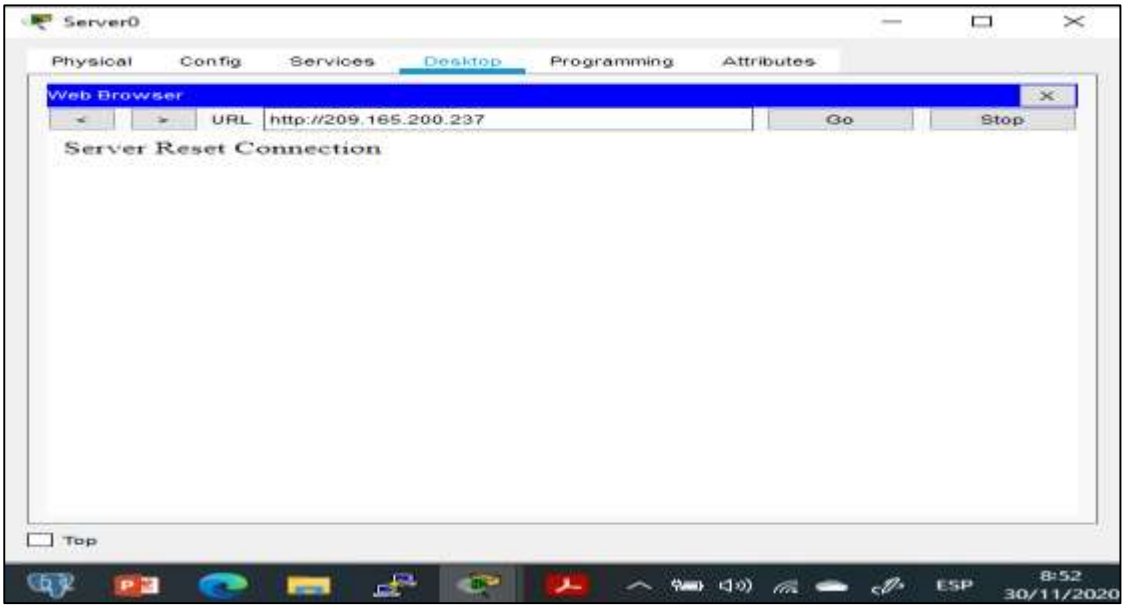
Fuente Propia

Figura 39. Ping PC-A a PC-C



Fuente propia

Figura 40. Acceso al servidor web



Fuente propia

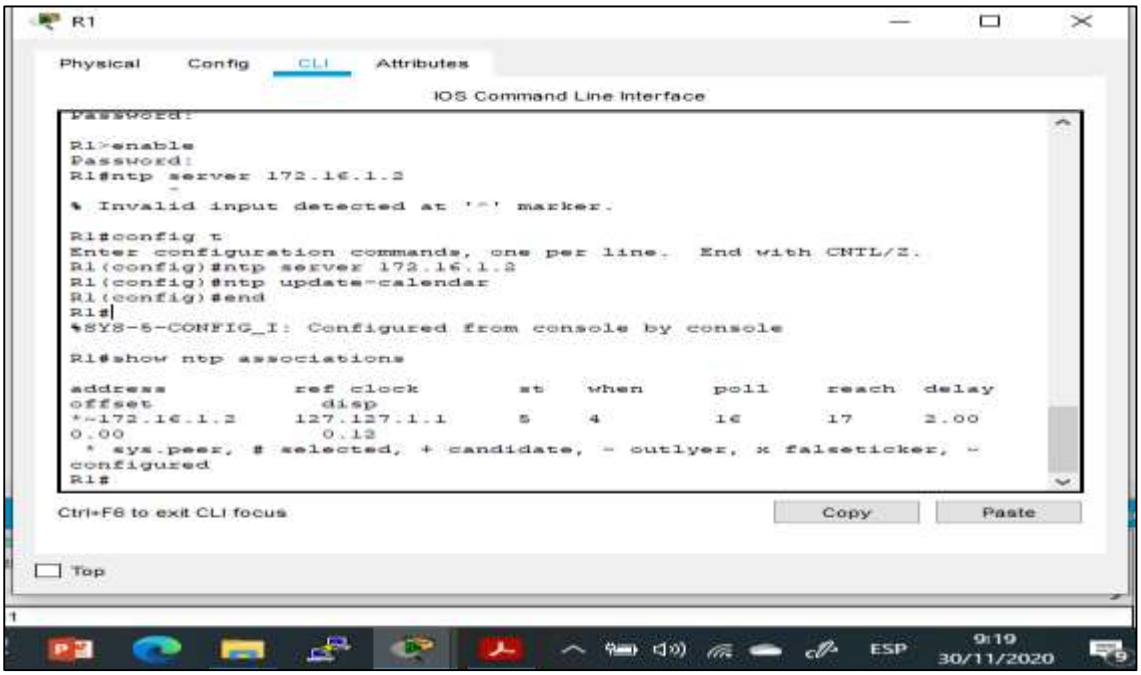
2.6 Configuración de NTP

Procedemos ahora a realizar la configuración de NTP, inicialmente se ajusta la fecha y hora, luego se configura a R2 como maestro NTP y a R1 como cliente NTP. Finalmente, verificamos en la configuración de NTP en R1.

Tabla 30. Configuración NTP en R2 y R1

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 09:10:00 05 November 2020
Configure R2 como un maestro NTP.	R2#config t R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1#config t R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#end
Verifique la configuración de NTP en R1.	R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 4 16 17 2.00 0.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Figura 41. Verificación de la configuración de NTP en R1



Fuente propia

2.7 Configuración y verificación de las listas de control de acceso (ACL)

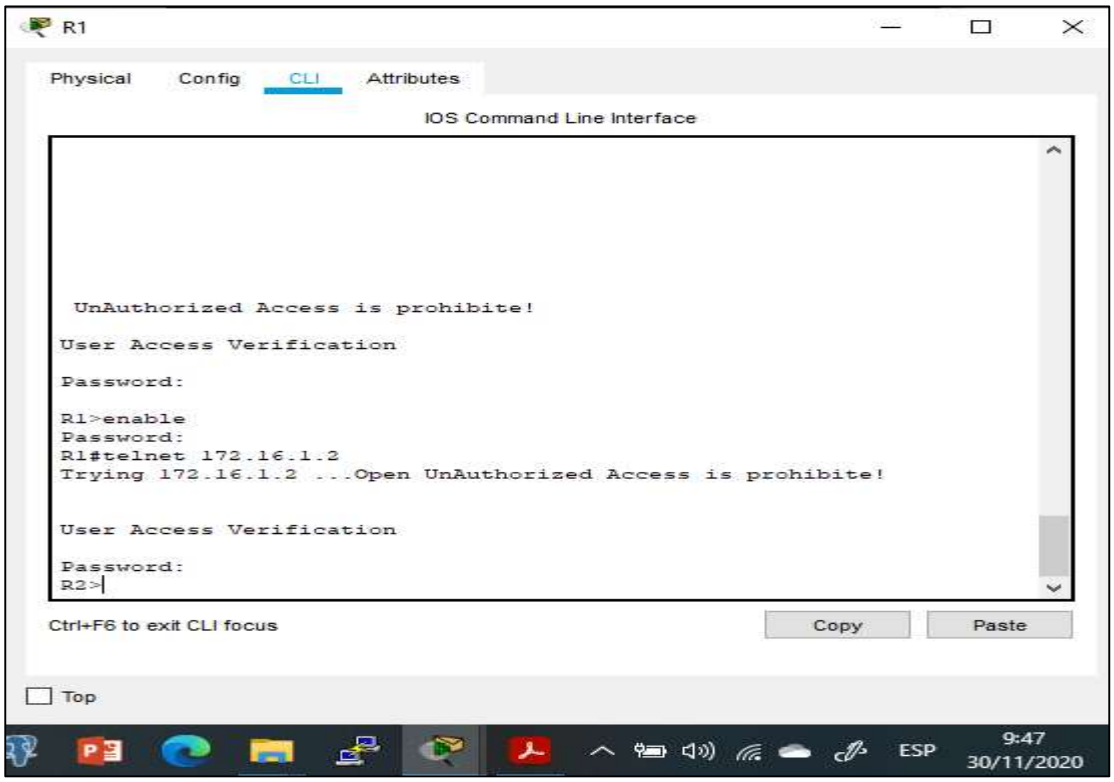
2.7.1 Restringir el acceso a las líneas VTY en el R2

Procedemos a configurar las listas control de acceso (ACL), permitiendo que solo R1 establezca una conexión Telnet con R2, restringiendo todo acceso a las líneas VTY. Luego realizamos la verificación de las configuraciones a través de los comandos detallados en la siguiente tabla:

Tabla 31. Configuración y verificación de ACL

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 t 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	Satisfactorio

Figura 42. Verificación de ACL en R1



Fuente propia

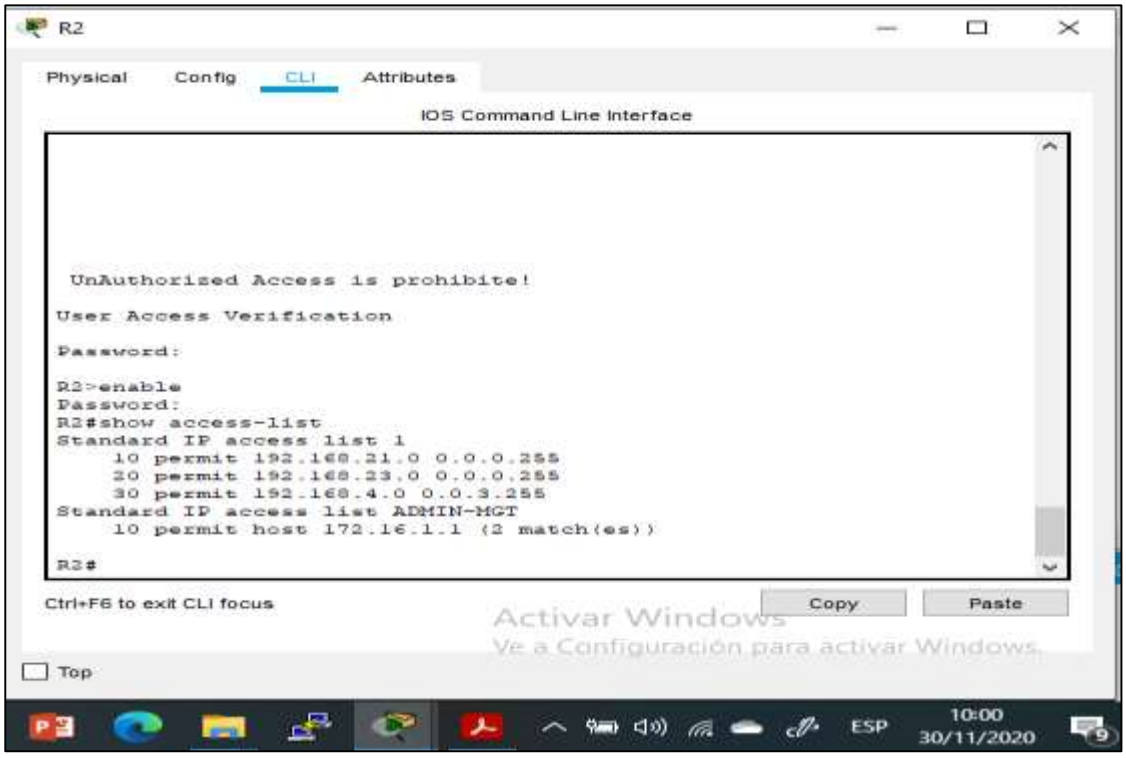
2.7.2 Introducción del comando de CLI adecuado que se necesita para verificar listas ACL.

Tabla 32. Verificación de las listas de acceso ACL

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

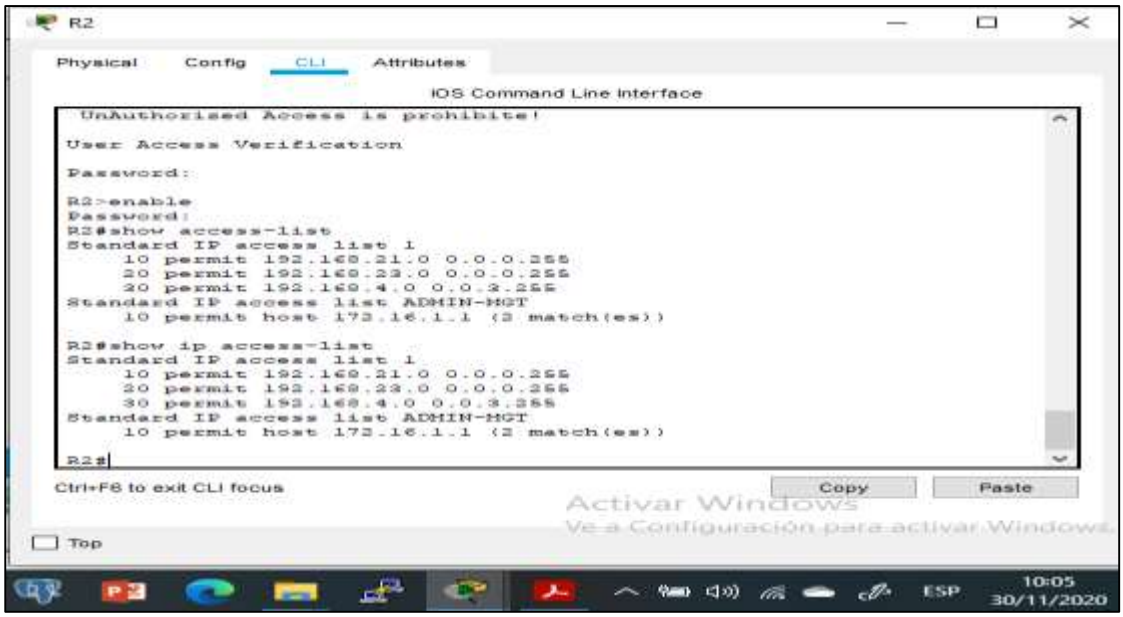
Restablecer los contadores de una lista de acceso	R2#show ip access-list R2#clear access-list counters R2#clear ip ? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries
¿Qué comando se usa para mostrar qué ACL se aplica 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 *

Figura 43. Show access list en R2



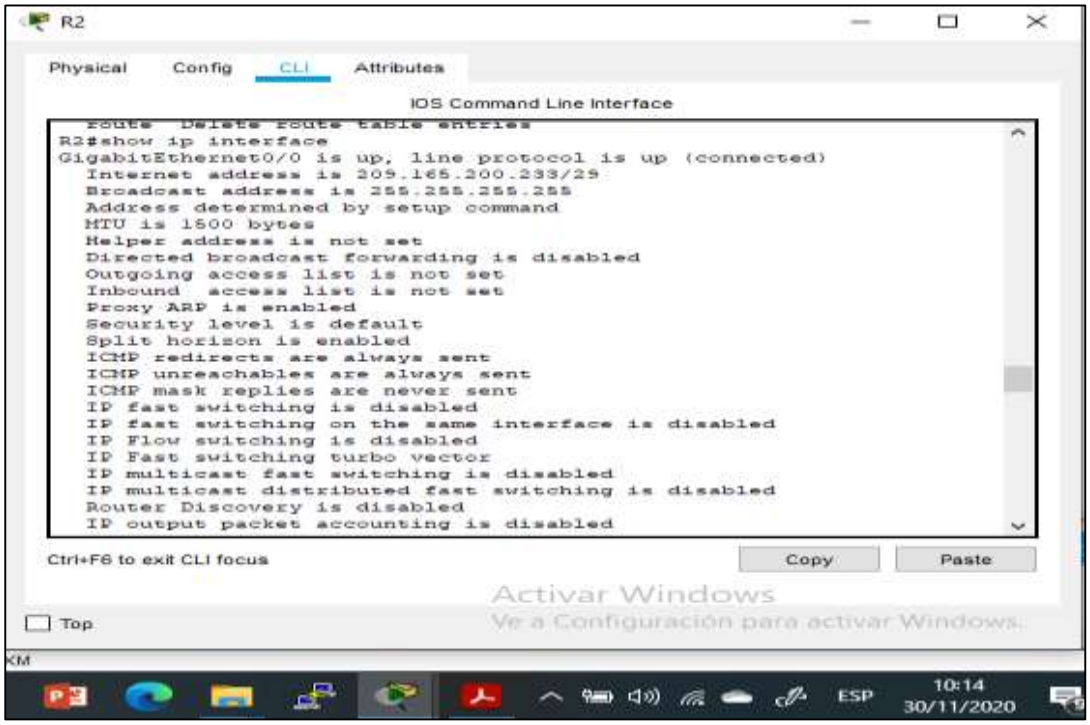
Fuente propia

Figura 44. Show ip access list en R2



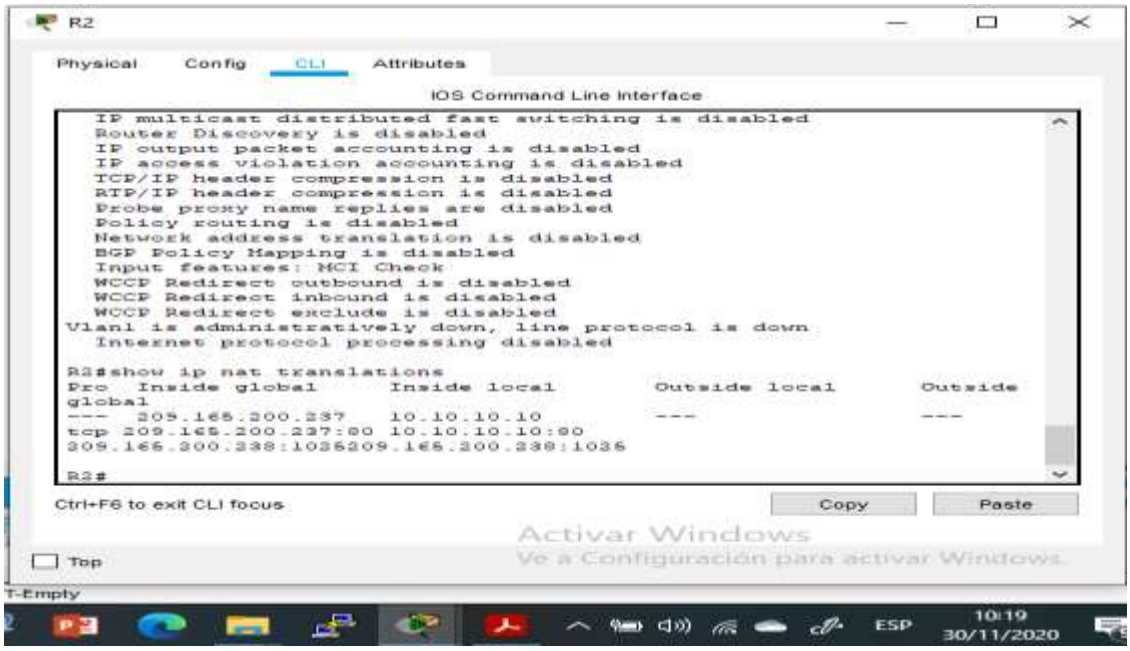
Fuente propia

Figura 45. show ip interface en R2



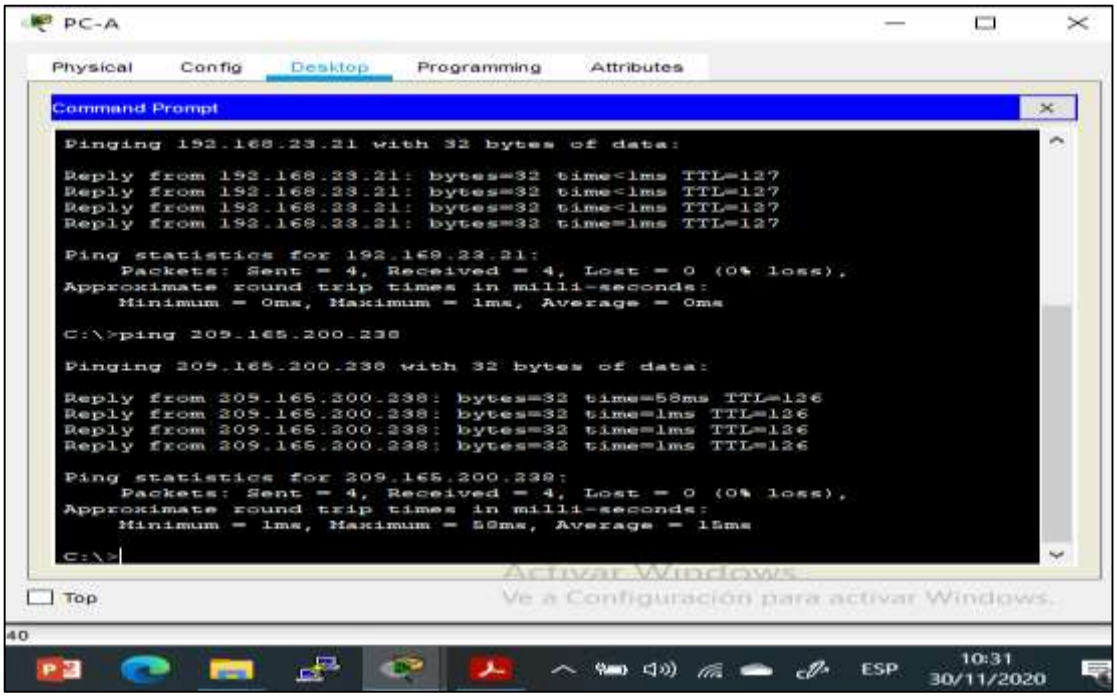
Fuente propia

Figura 46. Show ip nat translations en R2



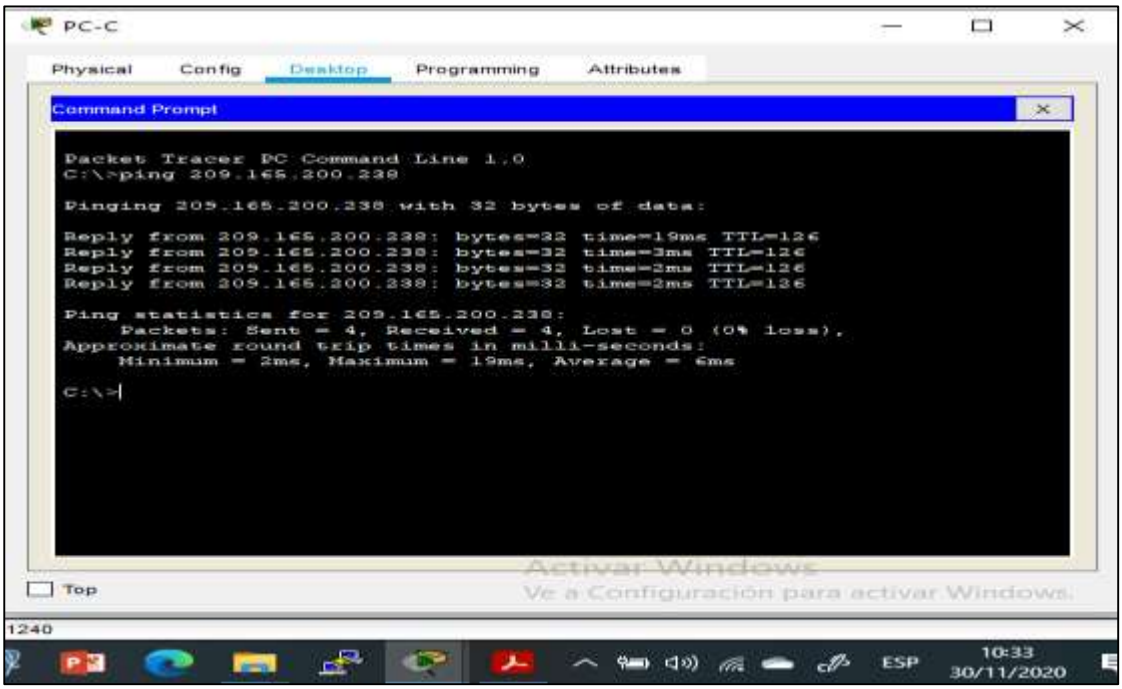
Fuente propia

Figura 47. Ping desde PC-A a Servidor



Fuente propia

Figura 48. Ping desde PC-C a Servidor



Fuente propia

Anexos

Link de ejercicios

https://drive.google.com/drive/folders/1hbAAD4bdTHD4vIczz8_phkgRY0m41N3h?usp=sharing

Link de Artículo Científico

https://drive.google.com/drive/folders/1PyySu0JaGtbOv0KnBUH3E5cc92CPIrkU?usp=sharing

Artículo Científico

Solución de un escenario presente en entornos corporativos bajo el uso de tecnología CISCO (noviembre de 2020)

Dahianna Vanesa Ospina

Resumen - Teniendo en cuenta el papel que desempeña en la actualidad la tecnología en el desarrollo global de la economía a nivel mundial, hace que cada vez más las Organizaciones inviertan en una arquitectura tecnológica segura y robusta, que le permitan garantizar la seguridad, confiabilidad y disponibilidad de la información.

Es por ello que los escenarios de redes requieren un diseño basado en la implementación de protocolos de seguridad que garanticen una conectividad optima entre sus dispositivos, permitan restricción de comunicación no requerida, métricas de enrutamiento, análisis de tráfico y autenticación de seguridad que brinden confidencialidad de los datos que circulan a través de la red.

Haciendo uso de la herramienta de simulación PACKET TRACER, de CISCO Networking Academy, se lleva a cabo la práctica de los conocimientos adquiridos, mediante el desarrollo de dos escenarios, que plantean la configuración de redes pequeñas, que deben permitir conectividad IPv4 e IPv6, implementando configuraciones básicas de seguridad, enrutamiento entre VLAN, DHCP, Etherchannel y port-security, 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.

Palabras Claves – VLAN, DNS, OSPF, PING.

I. INTRODUCCION

Mediante el desarrollo del presente trabajo que busca afianzar los conocimientos adquiridos en el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN), a través de la configuración de dos escenarios: El primero corresponde a una pequeña red, debe admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados, el router y los switches deben administrarse de forma segura, realizándose configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security. En el segundo escenario se implementa 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.

Teniendo en cuenta que uno de los factores más primordiales en el diseño de una red es garantizar seguridad y disponibilidad, se hace necesario la configuración adecuada de los dispositivos de red, a través de la implementación de protocolos seguros que permitan la comunicación necesaria y denieguen la no requerida, filtrando el tráfico de red para optimizar los recursos, permitiendo análisis de comportamiento y métricas de enrutamiento, diseñando políticas de enrutamiento estático y/o dinámico (RIP y OSPF), bajo un esquema de direccionamiento IP sin clase, que permite dar soluciones de red y conectividad escalables, a través del uso de enrutamiento y conmutación de paquetes en redes LAN y WAN

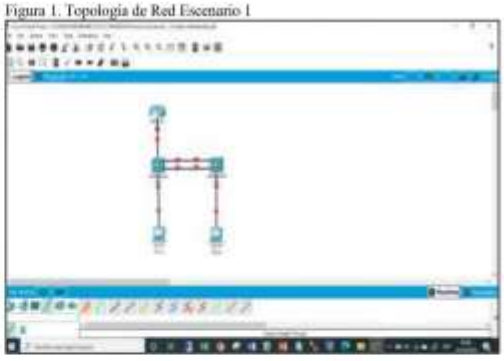
Documento Presentado el 30 de noviembre de 2020. Este trabajo fue direccionado por la Universidad Nacional Abierta y a Distancia Escuela de Ciencias Básicas Tecnologías e Ingenierías, Ingeniería de Sistemas (Asesor Ing. Juan Carlos Vesga Ferreira).

II. METODOLOGÍA

A. *Topología de Red*

Con base en la topología de red propuesta, se procede a realizar la configuración física del primer escenario, el cual corresponde a una pequeña red, en la que se realiza la configuración de los dispositivos: Un router, dos switch y dos equipos PC los cuales deben admitir tanto la conectividad IPv4 como IPv6 para los hosts soportados. Igualmente, el router y los switches deben administrarse de forma segura, permitir la configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Figura 1. Topología de Red Escenario 1



B. *Configuración de Dispositivos*

Según los requerimientos del Escenario 1, se procede a realizar la configuración inicial de cada uno de los dispositivos como primer paso, borrar las configuraciones de inicio del router y de los switches, así como las VLAN y se vuelven a cargar los dispositivos, verificando con el mensaje arrojado por los dispositivos que no tienen configuración de inicio, posteriormente se realiza la configuración de la plantilla SDM verificando que admita IPv6 según sea necesario y se vuelven a cargar los switches. Estas tareas se llevan a cabo mediante el uso de los comandos descritos en la siguiente tabla.

Tabla 1. Borrado de Configuración inicial

Tarea	Comando
Borrar las configuraciones de inicio en el Router	Router>enable Router#erase startup-config
Volver a cargar el router	Router#reload
Borrar las configuraciones de inicio en los Switches	Switch>enable Switch#erase startup-config
Borrado de la Base de Datos de la VLAN en los switches	Switch#delete vlan.dat
Volver a cargar los switches	Switch#reload
Configuración de la plantilla SDM para que admita IPv6 en los switches	Switch>enable Switch#show sdm prefer

Configuración de R1

Posterior a la inicialización de los dispositivos, se procede a realizar la configuración básica de seguridad del Router, que incluye las tareas descritas en la en la siguiente tabla:

Como primera medida se desactiva la búsqueda de DNS, luego se asigna en el nombre al router en este caso R1, se asigna un nombre de dominio y se establecen las contraseñas de acceso privilegiado, de consola con una longitud mínima de 10 caracteres y de inicio de sesión en las líneas VTY, se crea el usuario administrador en la base de datos local, se configura VTY solo aceptando la conexión segura SSH, se cifran las contraseñas y se configura el mensaje de acceso prohibido no autorizado.

Posteriormente procedemos a habilitar el Routing-ipv6 para enrrutar paquetes IPv6 entre las interfaces del Router. Continuamos con la Configuración de las interfaces y sus subinterfaces desde el modo de configuración global, habilitando la encapsulación IEEE 802.1Q del tráfico en cada una de ellas, basados en la tabla de direcciones ip se asigna la descripción a cada una de ellas y se activan las interfaces. Finalmente se configura la interface Loopback. y se genera una clave de cifrado RSA.

Tabla 2. Configuración de R1

Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las lineas 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 R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd # UnAuthorized Access is prohibite!#
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)# 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)#description Management 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
Configure el Loopback0 interface	R1(config-if)#int loopback 0 R1(config-if)#ip addres 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 R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa modulus 1024 (comando invalido en packet tracer) R1(config)#crypto key generate rsa

Configuración de S1 y S2

Se realiza las configuraciones básicas de seguridad en los switches, se asignan los nombres según la topología (S1 y S2), se desactiva la búsqueda DNS, se asignan las contraseñas de acceso privilegiado, de consola y telnet: ciscoenpass, se crea el mensaje de acceso no autorizado, se configura VTY solo aceptando la conexión segura SSH, se configuran las VLAN, acorde con la tabla de direccionamiento IPV4 e IPV6, se genera una clave de cifrado RSA, se configura la interfaz de administración (SVI) y se configura el gateway predeterminado, tareas que se detallan en la siguiente tabla:

Tabla 3. Configuración de S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config term Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
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 ciscoenpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	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 S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd # UnAuthorized Access is prohibite!#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa modulus 1024(comando invalido en packet tracer)
	S1(config)#crypto key generate rsa
Configurur 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 S1(config)#ipv6 route ::/0 2001:db8:acad:c::1

Se procede a crear las VLAN, asignando sus nombres conforme a la topología de red, VLAN 2 (Bikes), VLAN 3 (Trikes), VLAN 4 (Management), VLAN 5 (parking) y VLAN 6 (Native), se realiza la configuración de las conexiones troncales que utilicen la VLAN 6 nativa en la interfaz g1/0/5 y g1/0/1-2, luego procedemos a crear el grupo de puertos EtherChannel de Capa 2 que use las interfaces F0/1 y F0/2, por la interfaz g1/0/6 se configura el puerto de acceso de host para VLAN 2, se configuran los puertos de acceso de los Switch para conexión de los Host y se activan a las VLAN las interfaces fa0/6 y fa0/18, de acuerdo a las conexiones de los host en cada switch. Finalmente se configura la seguridad en los puertos de acceso y se procede a apagar los puertos no utilizados. Según la tabla de equivalencias propuesta para la topología de red.

Tabla 4. Configuración de VLAN en S1

Tarea	Especificación
Crear VLAN	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)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	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 S1(config-if)#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)#interface 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	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
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 S1(config)#int range g1/0/1-2 S1(config-if-range)#no shutdown

Configuración soporte de host

Acorde a las indicaciones del escenario se procede a realizar el enrutamiento por defecto en R1 y la creación de rutas predeterminadas para IPv4 e IPv6 para direccionar tráfico a la interfaz Loopback 0, creación de un grupo DHCP para VLAN 2 y VLAN 3 compuesto por las últimas 10 direcciones utilizables de la subred, identificando la dirección BROADCAST en cada subinterface y creación del nombre de dominio, conforme a la tabla de direccionamiento.

Se procede con la activación del servicio DHCP y se asigna el nombre al Pool de direccionamiento y la puerta de enlace predeterminada. Adicionalmente se asigna el DNS y se excluyen las direcciones, verificando que se habiliten las últimas 10 direcciones de la subred en cada VLAN.

Configuración de Enrutamiento

Tabla 5. Configuración de Enrutamiento R1

Tarea	Especificación
Configure Default Routing	R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp 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)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 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 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Configuración de los PC

Se realiza la configuración física de los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asignen estáticamente las direcciones IPv6 GUA y Link Local. Después de realizar la configuración en cada PC, se procede a verificar las configuraciones de red de cada host usando el comando ipconfig /all, evidenciándose la configuración de red acorde a la topología y los requerimientos del escenario propuesto, descripciones que se detallan en las tablas No. 6 y No. 7, Dirección física, Dirección IP, Máscara de subred, Gateway predeterminado y Gateway predeterminado IPv6.

Figura 2. Asignación Estática de IPV6 y link Local PC-A

Se realiza la asignación Estática de IPV6 y link Local en el PC-A conforme a los parámetros establecidos en la tabla de direccionamiento y se procede con la respectiva verificación de la configuración a través de la ejecución del comando ipconfig /all.

Figura 3. Configuración de red host PC-A

Tabla 6. Detalle de configuración de red host PC-A

PC-A Network Configuration	
Descripción	
Dirección física	0001.97C7.6711
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 4. Asignación Estática de IPV6 y link Local PC-B

Se realiza la asignación Estática de IPV6 y link Local en el PC-B conforme a los parámetros establecidos en la tabla de direccionamiento y se procede con la respectiva verificación de la configuración a través de la ejecución del comando ipconfig /all,

Figura 5. Configuración de red host PC-B

Tabla 7. Detalle de configuración de red host PC-B

PC-A Network Configuration	
Descripción	
Dirección física	0000.0C5A.4D5B
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

C. Probar y verificar la conectividad de extremo a extremo

Haciendo uso del comando ping, se procede a probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red, verificaando los resultados de forma satisfactoria de las peticiones de los Host (PC-A y PC-B) a cada una de las interfaces del Router y los Switchs. Según requerimientos detallados en la siguiente tabla.

Tabla 8. Verificación de Conectividad entre dispositivos

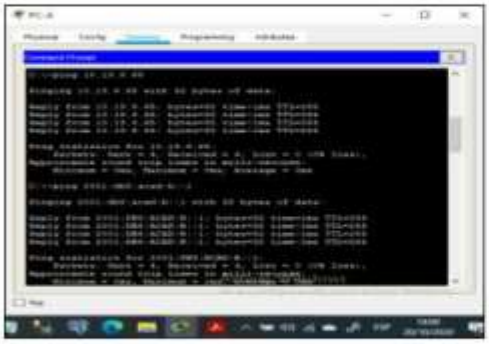
Desde	A	de Internet	Dirección IP
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1
		IPv6	2001:db8:acad:a: :1
	R1, G0/0/1.3	Dirección	10.19.8.65
		IPv6	2001:db8:acad:b::1
	R1, G0/0/1.4	Dirección	10.19.8.97
		IPv6	2001:db8:acad:c::1
	S1, VLAN 4	Dirección	10.19.8.98
		IPv6	2001:db8:acad:c::98
	S2, VLAN 4	Dirección	10.19.8.99
		IPv6	2001:db8:acad:c::99
	PC-B	Dirección	10.19.8.86
		IPv6	2001:db8:acad:b::50
	R1 Bucle 0	Dirección	209.165.201.1
		IPv6	2001:db8:acad:209: :1
PC-B	R1 Bucle 0	Dirección	209.165.201.1
		IPv6	2001:db8:acad:209::1
	R1, G0/0/1.2	Dirección	10.19.8.1
		IPv6	2001:db8:acad:a: :1
	R1, G0/0/1.3	Dirección	10.19.8.65
		IPv6	2001:db8:acad:b: :1
	R1, G0/0/1.4	Dirección	10.19.8.97
		IPv6	2001:db8:acad:c: :1
	S1, VLAN 4	Dirección	10.19.8.98
		IPv6	2001:db8:acad:c: :98
	S2, VLAN 4	Dirección	10.19.8.99.
		IPv6	2001:db8:acad:c: :99

Obteniendose resultados satisfactorios en la conectividad, como se evidencia en la ejecucion del comando ping en las siguientes imágenes.

Figura 6. Ping desde PC-A a R1, G0/0/1.2

Se evidencia conectividad satisfactoria entre el PC-A y R1 en la interfaz G0/0/1.2. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 7. Ping desde PC-A a R1, G0/0/1.3



Se evidencia conectividad satisfactoria entre el PC-A y R1 en la interfaz G0/0/1.3. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 8. Ping desde PC-A a R1, G0/0/1.4

Se evidencia conectividad satisfactoria entre el PC-A y R1 en la interfaz G0/0/1.4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 9. Ping desde PC-A a S1, VLAN 4

Se evidencia conectividad satisfactoria entre el PC-A y S1-VLAN 4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 10. Ping desde PC-A a S2, VLAN 4

Se evidencia conectividad satisfactoria entre el PC-A y S2-VLAN 4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 11. Ping desde PC-A a PC-B

Con el anterior ping, se evidencia conectividad satisfactoria entre el PC-A y PC-B. Resultado que refleja una adecuada configuracion en el direccionamiento de la red y por consiguiente se verifica que existe conectividad de extremo a extremo.

Figura 12. Ping desde PC-A a R1, Bucle 0

Se evidencia conectividad satisfactoria entre el PC-A y R1 Bucle 0. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 13. Ping desde PC-B a R1, Bucle 0

Se evidencia conectividad satisfactoria entre el PC-B y R1 Bucle 0. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 14. Ping desde PC-B a R1, G0/0/1.2

Se evidencia conectividad satisfactoria entre el PC-B y R1 en la interfaz G0/0/1.2. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 15. Ping desde PC-B a R1, G0/0/1.3

Se evidencia conectividad satisfactoria entre el PC-B y R1 en la interfaz G0/0/1.3. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 16. Ping desde PC-B a R1, G0/0/1.4

Se evidencia conectividad satisfactoria entre el PC-B y R1 en la interfaz G0/0/1.4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red.

Figura 17. Ping desde PC-B a S1, VLAN 4

Se evidencia conectividad satisfactoria entre el PC-B y S1-VLAN 4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red

Figura 18. Ping desde PC-B a S2, VLAN 4

Se evidencia conectividad satisfactoria entre el PC-B y S2-VLAN 4. Resultado que refleja una adecuada configuracion en el direccionamiento de la red

III. CONCLUSIONES

Los protocolos de enrutamiento determinan cuál es la ruta más corta que deben seguir el router para enviar los datos.

La implementación de los protocolos de enrutamiento permite definir políticas de seguridad, establecer la comunicación entre los diferentes dispositivos de una red, así mismo garantizan, confiabilidad y disponibilidad de los datos.

La implementación de VLAN permite optimizar el tráfico de la red y una mayor seguridad, dado que separan la red, lo cual disminuye la ocurrencia de ataques.

Siempre que se inicia la configuración básica de los dispositivos de una red, es necesario realizar el borrado de configuraciones de inicio y el reinicio de los dispositivos con el objetivo de permitir una óptima configuración de los mismos acordes al escenario planteado.

El comando ping permite verificar la conectividad entre los dispositivos de la red.

En el diseño de la topología de red, es fundamental verificar el requerimiento de puertos seriales a utilizar en los routers, tipos de dispositivos a utilizar, cableado de red requerido y la comunicación permitida y denegada.

REFERENCIAS

[1] CISCO. CCNA Exploration. Conceptos y protocolos de enrutamiento. Cuarta version. México. CISCO NETWORKING ACADEMY, 2011.

[2] "Listas de Control de Acceso". CISCO (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourse- assets.s3.amazonaws.com/RSE6/es/index.html#7

[3] LÓPEZ BULLA, Ricardo. "Enrutamiento y configuración de redes: Fundación Universitaria del Área Andina" {En línea}. {10 septiembre de 2018} disponible en: (https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACI%C3%93N%20DE%20REDES.pdf?sequence=1&isAllowed=y)

[4] PRIETO FERNANDEZ, Raúl. "Enrutamiento dinámico OSPF con Packet Tracer: My Blog" {En línea}. {20 agosto de 2016} disponible en: (https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamicoospf- con-packet-tracer)

[5] RAMOS GATA, Jose Ramón. "Vlan: Ragasys Sistemas" {En línea}. {30 junio de 2020} disponible en: (https://blog.ragasys.es/tag/vlan)

[6] PRIETO FERNANDEZ, Raúl. "Enrutamiento entre VLANS con Packet Tracer: My Blog" {En línea}. {12 junio de 2019} disponible en: (https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-entre-vlans-con-packet-tracer)

[7] DI TOMMASO, Leandro. "configuración de VLANS con CISCO: Micro Ways" {En línea}. {6 agosto de 2009} disponible en: (https://www.mikroways.net/2009/08/05/configuracion-de-vlans-con-cisco/)

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

[9] INFOTECS "Arquitectura de Redes Seguras" {En línea}. {27 enero de 2020} disponible en: (https://infotecs.mx/blog/arquitectura_de_redes_seguras.html)

[10] DEL BARRIO DAVID. " Enrutamiento" {En línea}. {22 marzo de 2019} disponible en: https://eltallerdelbit.com/enrutamiento-fundamentos-y-protocolos/).

Conclusiones

Los protocolos de enrutamiento determinan cuál es la ruta más corta que deben seguir el router para enviar los datos.

La implementación de los protocolos de enrutamiento permite definir políticas de seguridad, establecer la comunicación entre los diferentes dispositivos de una red, así mismo garantizan, confiabilidad y disponibilidad de los datos.

La implementación de VLAN permite optimizar el tráfico de la red y una mayor seguridad, dado que separan la red, lo cual disminuye la ocurrencia de ataques.

Siempre que se inicia la configuración básica de los dispositivos de una red, es necesario realizar el borrado de configuraciones de inicio y el reinicio de los dispositivos con el objetivo de permitir una óptima configuración de los mismos acordes al escenario planteado.

El comando ping permite verificar la conectividad entre los dispositivos de la red.

En el diseño de la topología de red, es fundamental verificar el requerimiento de puertos seriales a utilizar en los routers, tipos de dispositivos a utilizar, cableado de red requerido y la comunicación permitida y denegada.

Bibliografía

CISCO. CCNA Exploration. Conceptos y protocolos de enrutamiento. Cuarta version. México. CISCO NETWORKING ACADEMY, 2011.

RAMOS GATA, Jose Ramón. "Vlan: Ragasys Sistemas" {En línea}. {30 junio de 2020} disponible en: (https://blog.ragasys.es/tag/vlan).

NAT (Network Address Translation. (2020, 9 junio). Tomado de Wikipedia. https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

"Listas de Control de Acceso". CISCO (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://staticcourse-assets.s3.amazonaws.com/RSE6/es/index.html#7

LÓPEZ BULLA, Ricardo. "Enrutamiento y configuración de redes: Fundación Universitaria del Área Andina" {En línea}. {10 septiembre de 2018} disponible en: (https://digitk.areandina.edu.co/bitstream/handle/areandina/1495/74%20ENRUTAMIENTO%20Y%20CONFIGURACI%C3%93N%20DE%20REDES.pdf?sequence=1&isAllowed=y)